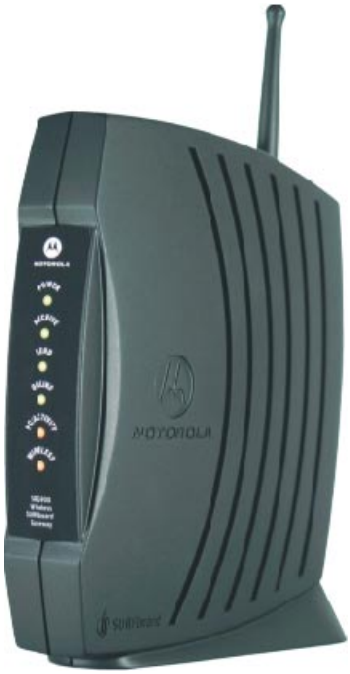
User Guide

SBG900
Wireless Cable
Modem Gateway

MOTOROLA
intelligence everywhere™



WARNING: TO PREVENT FIRE OR SHOCK HAZARD, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. THE UNIT MUST NOT BE EXPOSED TO DRIPPING OR SPLASHING. DO NOT PLACE OBJECTS FILLED WITH LIQUIDS, SUCH AS VASES, ON THE UNIT.

CAUTION: TO ENSURE REGULATORY AND SAFETY COMPLIANCE, USE ONLY THE PROVIDED POWER AND INTERFACE CABLES. DO NOT CONNECT THE PLUG INTO AN EXTENSION CORD, RECEPTACLE, OR OTHER OUTLET UNLESS THE PLUG CAN BE FULLY INSERTED WITH NO PART OF THE BLADES EXPOSED.

CAUTION: DO NOT OPEN THE UNIT. DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE INSTALLATION AND TROUBLESHOOTING INSTRUCTIONS. REFER ALL SERVICING TO QUALIFIED SERVICE PERSONNEL.

CAUTION: CHANGES AND MODIFICATIONS NOT EXPRESSLY APPROVED BY MOTOROLA FOR COMPLIANCE COULD VOID USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

CAUTION: Exposure to Radio Frequency Radiation. To comply with the FCC RF exposure compliance requirements, the separation distance between the antenna and any person's body (including hands, wrists, feet and ankles) must be at least 8 inches (20 cm).

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product.

Postpone cable modem installation until there is no risk of thunderstorm or lightning activity in the area.

Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.

Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the product.

Place this equipment in a location that is close enough to an electrical outlet to accommodate the length of the power cord.

Place this equipment on a stable surface.

Be sure that the outside cable system is grounded, so as to provide some protection against voltage surges and built-up static charges. Article 820-20 of the NEC (Section 54, Part I of the Canadian Electrical Code) provides guidelines for proper grounding and, in particular, specifies the CATV cable ground shall be connected in the grounding system of the building, as close to the point of cable entry as practical.

When using this device, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Read all of the instructions {listed here and/or in the user manual} before you operate this equipment. Give particular attention to all safety precautions. Retain the instructions for future reference.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this equipment.
- Comply with all instructions that accompany this equipment.
- *Avoid using this product during an electrical storm.* There may be a risk of electric shock from lightning. For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet, and disconnect the cable system. This will prevent damage to the product due to lightning and power surges.
- Avoid damaging the cable modem with static by touching the coaxial cable when it is attached to the earth grounded coaxial cable TV wall outlet.
- Always first touch the coaxial cable connector on the cable modem when disconnecting or re-connecting USB or Ethernet cable from the cable modem or the user's PC.
- Operate this product only from the type of power source indicated on the product's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in safe operating condition.

It is recommended that the customer install an AC surge protector in the AC outlet to which this device is connected. This is to avoid damaging the equipment by local lightning strikes and other electrical surges.

Different types of cord sets may be used for connections to the main supply circuit. Use only a main line cord that complies with all applicable product safety requirements of the country of use.

Installation of this product must be in accordance with national wiring codes.

Place unit to allow for easy access when disconnecting the power cord/adapter of the device from the AC wall outlet.

Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.

This product was qualified under test conditions that included the use of the supplied cables between system components. To be in compliance with regulations, the user must use these cables and install them properly. Connect the unit to a grounding type AC wall outlet using the power adapter supplied with the unit.

Do not cover the device, or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.

Installation must at all times conform to local regulations.

This product is provided with a separate *Regulatory, Safety, Software License, and Warranty Information* card. If one is not provided with this product, please ask your service provider or point-of-purchase representative, as the case may be.

- THIS PRODUCT IS IN COMPLIANCE WITH ONE OR MORE OF THE STANDARDS LISTED ON THE *REGULATORY, SAFETY, SOFTWARE LICENSE, AND WARRANTY INFORMATION* CARD. NOT ALL STANDARDS APPLY TO ALL MODELS.
- NO WARRANTIES OF ANY KIND ARE PROVIDED BY MOTOROLA WITH RESPECT TO THIS PRODUCT, EXCEPT AS STATED ON THE *REGULATORY, SAFETY, SOFTWARE LICENSE, AND WARRANTY INFORMATION* CARD. MOTOROLA'S WARRANTIES DO NOT APPLY TO PRODUCT THAT HAS BEEN REFURBISHED OR REISSUED BY YOUR SERVICE PROVIDER.

Copyright © 2003 by Motorola, Inc.

All rights reserved. No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation or adaptation) without written permission from Motorola, Inc.

Motorola reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of Motorola to provide notification of such revision or change. Motorola provides this guide without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Motorola may make improvements or changes in the product(s) described in this manual at any time.

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. Microsoft, Windows, Windows Me, and Windows NT are registered trademarks and Windows XP is a trademark of Microsoft Corporation. Microsoft Windows screen shots are used by permission of Microsoft Corporation. Macintosh and AppleTalk are registered trademarks of Apple Computer, Inc. Iomega is a registered trademark of Iomega Corporation. Linux is a registered trademark of Linus Torvalds. Acrobat Reader is a registered trademark of Adobe Systems, Inc. Netscape and Navigator are registered trademarks of Netscape Communications Corporation. UNIX is a registered trademark of the Open Group in the United States and other countries. All other product or service names are the property of their respective owners. © Motorola, Inc. 2003.

Contents

Overview 1
Easy Setup 2
Network Connection Types 2
Powerful Features in a Single Unit 3
Sample LAN 4
Optional Accessories 5
Front Panel 6
Rear Panel 7
Label on the Bottom of the SBG900 8
SBG900 LAN Choices 8
Wireless LAN 9
Wired Ethernet LAN 10
USB Connection 11
Security 12
Firewall 12
DMZ 13
Port Triggering 13
Wireless Security 13
Port Forwarding 14
Virtual Private Networks 14
Related Documentation 14

Installation. 15
Before You Begin 15
Precautions 16
Signing Up for Service 16
Computer System Requirements 17
Connecting the SBG900 to the Cable System 18
Cabling the LAN 18
Obtaining an IP Address for Ethernet 19
Obtaining an IP Address in Windows 98, Windows 98 SE, or Windows Me 19
Obtaining an IP Address in Windows 2000 or Windows XP 19
Obtaining an IP Address on Macintosh or UNIX Systems 19
Connecting a PC to the USB Port 20

Basic Configuration 21
Starting the SBG900 Setup Program 22
Changing the Default Password 24
Enabling Remote Access 25
Getting Help 26
Setting the Firewall Policy 27
Firewall > POLICY — advanced Page 29
Firewall > ALERT — basic Page 31
Firewall > ALERT — email Page 32
Firewall > LOGS Page 33
Gaming Configuration Guidelines 35
Configuring the Firewall for Gaming 35
Configuring Port Triggers 35
Configuring a Gaming DMZ Host *36*

Configuring the Gateway 37
Gateway > STATUS Page 38
Gateway > WAN Page 39
Gateway > LAN — nat config Page 41
Gateway > LAN — dhcp server config Page 42
Gateway > LAN — dhcp leases Page 43
Gateway > PORT FORWARDING — status Page . . . 44
Gateway > PORT FORWARDING — config Page . . . 45
Gateway > PORT TRIGGERS — predefined Page . . 46
Gateway > PORT TRIGGERS — custom Page 48
Gateway > LOG Page 49

Configuring TCP/IP 50
Configuring TCP/IP in Windows 95, Windows 98, or Windows Me 51
Configuring TCP/IP in Windows 2000 53
Configuring TCP/IP in Windows XP 57
Verifying the IP Address in Windows 95, Windows 98, or Windows Me 61
Verifying the IP Address in Windows 2000 or Windows XP . 62

Setting Up the Wireless LAN 64
Configuring the Wireless Network Name on the SBG900 .65
Configuring WEP on the SBG900 67
Configuring a MAC Access Control List on the SBG900 . .68
Configuring the Wireless Clients 69
Configuring a Wireless Client with a Network Name (ESSID) 69
Configuring a Wireless Client for WEP 69
Wireless Pages in the SBG900 Setup Program 70
Wireless > STATUS Page 71
Wireless > NETWORK Page 72
Wireless > SECURITY — basic Page 74
Wireless > SECURITY — advanced Page 75
Wireless > STATISTICS page 76

Setting Up a USB Driver 78
Setting Up a USB Driver in Windows 98 79
Setting Up a USB Driver in Windows 2000 83
Setting Up a USB Driver in Windows Me 86
Setting Up a USB Driver in Windows XP 87
Removing the USB Driver from Windows 98 or Windows Me 88
Removing the USB Driver from Windows 2000 91
Removing the USB Driver from Windows XP 94

Troubleshooting 99
Front-Panel Lights and Error Conditions 99

Contact Us 100

Frequently-Asked Questions 101

Specifications 103
General 103
Cable Modem 104

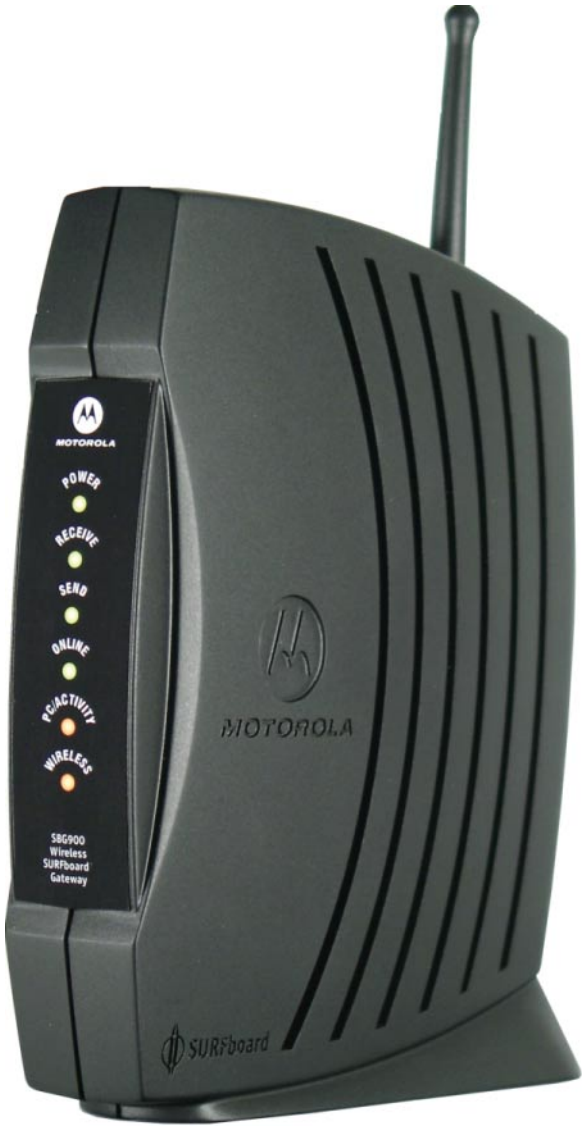
Glossary 105

Software License 123

Overview

Thank you for purchasing a Motorola® SURFboard® Wireless Cable Modem Gateway SBG900 for your home, home office, or small business/enterprise. Applications where the SURFboard Gateway (SBG) is especially useful include:

- Households having multiple computers requiring connection to the Internet and each other
- Small businesses or home offices requiring fast, affordable, and secure Internet access
- Internet gamers desiring easier setup for:
  - Programs such as DirectX® 7 or DirectX® 8
  - Sites such as MSN Games by Zone.com or Battle.net®
- Video conferencing



The features and physical appearance of your SBG900 may differ slightly from the picture.

Home networking enables you to access and move information between two or more computers in your home or business. Your home network connects to the cable TV system and enables you to connect to the Internet or other networks connected to the Internet. The SBG900 acts as the *central connection point* between your computers and the Internet. It directs (routes) computer data to the Internet and between your computers. A SURFboard cable modem in the SBG passes information between your home network computers and the Internet. An SBG900:

- Combines a SURFboard cable modem, IEEE 802.11g wireless access point, Ethernet 10/100Base-T connection, and an advanced firewall into one compact product
- Eliminates the need for four or five separate products, enabling you to maximize the potential of your existing resources
- Enables you to create a custom network sharing a single broadband connection, files, and other peripherals like scanners, with or without wires
- Offers enhanced network security for wired and wireless users
- Provides easy setup
- Enables cable operators to add future value-added services

This product is subject to change. Not all features described in this guide are available on all SBG900 models.

For the most recent documentation, visit the Product Documentation page on the Motorola Broadband website http://broadband.motorola.com/.

Easy Setup

It is much easier to configure a local area network (LAN) using an SBG900 than it is using typical networking equipment:

- The Installation Assistant application on the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM enables easy connection to the cable network.
- For basic operation, most default settings require no modification.
- The Setup Program provides a graphical user interface (GUI) for easy configuration of necessary wireless, Ethernet, router, DHCP, and security settings. For a list of issues, see “Basic Configuration”.

Network Connection Types

The SBG900 provides different network connection types for your computers to exchange data. The connection between your computers and the SBG900 may be with a wireless or a wired connection or a combination of the two. Your network can use one or any combination of all the following network connections:

- Ethernet local area network (LAN)
- Wireless LAN (IEEE 802.11g that also supports IEEE 802.11b devices)
- Universal Serial Bus (USB)

Powerful Features in a Single Unit

An SBG900 combines high-speed Internet access, networking, and computer security for a home or small-office LAN. An SBG900 provides:

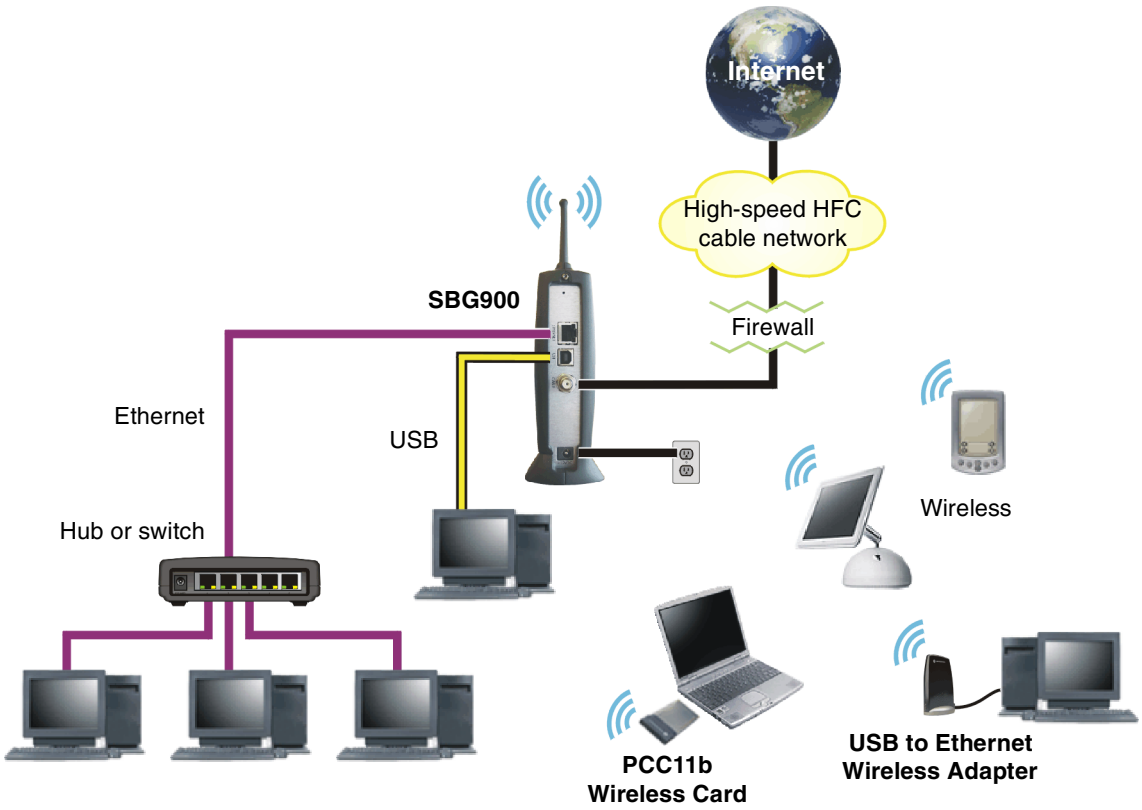
- An integrated high-speed SURFboard cable modem for continuous broadband access to the Internet and other online services, with much faster data transfer than traditional dial-up or ISDN modems
- A single broadband connection for up to 253 computers to surf the web; all computers on the LAN communicate as if they were connected to the same physical network
- An IEEE 802.11g wireless access point to enable laptop users to remain connected while moving around the home or small office or to connect desktop computers without installing network wiring. Depending on distance, wireless connection speeds can match that of Ethernet.
- A USB connection for a single PC
- A dual-purpose 10/100Base-T Ethernet uplink port supporting half- or full-duplex connections and Auto-MDIX
- Routing for a wireless LAN or a wired Ethernet LAN connected using a hub or switch
- A built-in DHCP server to easily configure a combined wired and/or wireless Class C private LAN
- An advanced firewall supporting stateful-inspection, intrusion detection, DMZ, denial-of-service attack prevention, and Network Address Translation (NAT)
- Virtual private network (VPN) pass-through operation supporting IPSec, PPTP, or L2TP to securely connect remote computers over the Internet
- Port Forwarding to configure ports to run applications having special network requirements

Sample LAN

The sample LAN shown in the figure contains the following devices, all protected by the SBG900 firewall:

- A PDA connected through the wireless connection
- One desktop Macintosh on a wireless connection
- One desktop PC on a wireless connection using a Motorola USB Adapter
- A laptop PC on a wireless connection connected using a Motorola PC Card
- One computer connected directly to Ethernet port one
- Three computers connected to Ethernet port two using a hub or switch
- One PC connected to the USB port

Sample SBG900 hybrid network



Optional Accessories

While any IEEE 802.11g or IEEE 802.11b compliant client product will work with the SBG900, Motorola has wireless adapters available for use with the SBG900.

You can use the Motorola PCC11b wireless card or the USB11b wireless adapter, which comply with the IEEE 802.11b wireless standard, to connect a PC to the wireless LAN:

USB11b Wireless Adapter

Connects a desktop, laptop, printer, or other peripheral device to the wireless LAN. It has a built-in antenna and a six feet (two meter) long cable that connects to the PC USB port. Its light indicates:

- Off — Not connected to a USB port or not receiving power from the PC
- Yellow — Not installed or initializing
- Green — Installed and operational
- Flashing Green — Receiving data from another wireless LAN device
- Flashing Yellow — Transmitting data to another wireless LAN device

PCC11b Wireless Card

A credit-card sized adapter that connects a laptop to the wireless LAN. You can roam in, or around, the home or small office and remain connected. It fits in a PCMCIA Type II standard slot on the laptop supporting 3.3 Volt PC card. The PCC11b has also has a built-in antenna.

Motorola USB11b Wireless Adapter (left) and PCC11b Wireless Card

For installation instructions, see the documentation provided with each product.

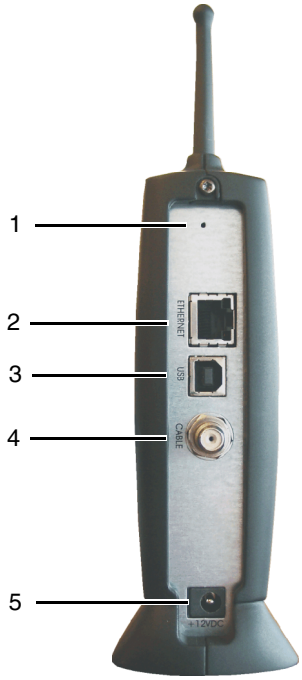
Front Panel

The front panel provides indicator lights. *The model number on your SBG may be different than in some illustrations and screen images.*

Key	Light	Flashing	On
1	**POWER**	None	The power supply is working properly
2	**RECEIVE**	Scanning for a receive (downstream) channel connection	The downstream channel is connected
3	**SEND**	Scanning for a send (upstream) channel connection	The upstream channel is connected
4	**ONLINE**	Scanning for a network connection	The startup process is complete and the SBG900 is online
5	**PC/ACTIVITY**	Transmitting or receiving data	A computer or other device is connected to the USB or Ethernet port
6	**WIRELESS**	Wireless activity	Wireless feature is functioning normally

Rear Panel

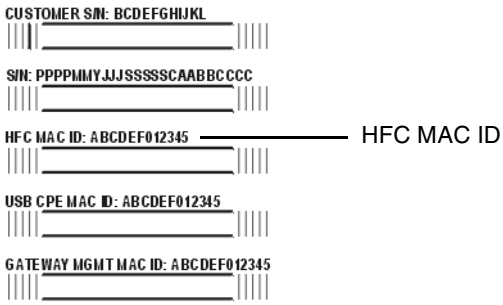
The rear panel provides cabling connectors, status lights, and the power receptacle:



Key	Item	Description
1	•	If you experience a problem, you can push this recessed button to restart the SBG900 (see "Troubleshooting"). To reset all values to their defaults, hold down the button for more than five seconds. Resetting may take 5 to 30 minutes because the SBG900 must find and lock on the appropriate communications channels.
2		Use the **ETHERNET** port to connect an Ethernet LAN cable with RJ-45 connectors to an Ethernet-equipped computer, hub, bridge, or switch.
3		For Windows *only*, use the **USB** port for Connecting a PC to the USB Port. You cannot connect the SBG900 USB port to a Macintosh or UNIX computer.
4		The **CABLE** port provides a connection to the coaxial cable outlet.
5		The **+12VDC** power connector to the external power supply.

Label on the Bottom of the SBG900

To receive data service, you need to provide the MAC address marked ***HFC MAC ID*** to your cable service provider*:*



SBG900 LAN Choices

The SBG900 enables connection of up to 253 client computers on a combination of:

- Wireless LAN
- Wired Ethernet LAN
- USB Connection

Each computer needs appropriate network adapter hardware and driver software. The clients on the Ethernet, wireless, or USB interfaces can share:

- Internet access with a single cable service provider account, subject to cable provider terms and conditions
- Files, printers, storage devices, multi-user software applications, games, and video conferencing

Wireless and wired network connections use Windows networking to share files and peripheral devices such as printers, CD-ROM drives, floppy disk drives, and Iomega® Zip Drives.

Wireless LAN

Wireless communication occurs over radio waves rather than a wire. Like a cordless telephone, a wireless LAN uses radio signals instead of wires to exchange data. A wireless network eliminates the need for expensive and intrusive wiring to connect computers throughout the home or office. Mobile users can remain connected to the network even when carrying their laptop to different locations in the home or office.

Each computer on a wireless LAN requires an adapter described in "Optional Accessories":

Laptop PCs Use a Motorola PCC11b Wireless Card in the PCMCIA slot.

Desktop PCs Use a Motorola USB11b Wireless Adapter to connect the USB port.

Sample wireless network connections

To set up the SBG900, on a computer wired to the SBG900 over Ethernet or USB, perform the procedures in "Setting Up the Wireless LAN". *Do not attempt to configure the SBG900 over a wireless connection.*

To set up each wireless client (station):

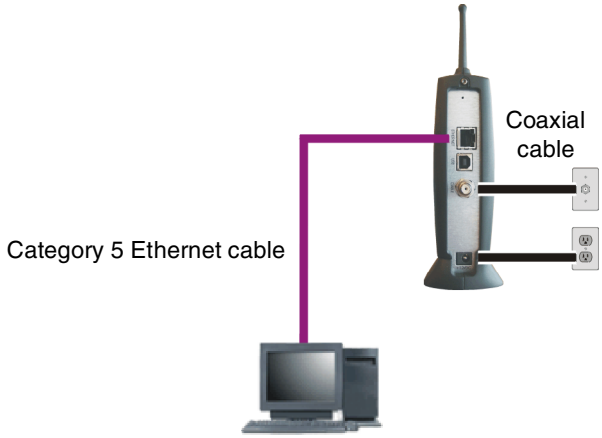
1. Insert the *PCC11b and USB11b Wireless Adapter* CD-ROM in the CD-ROM drive on the client.
2. Install the device software from the CD.
3. Connect the Motorola PCC11b wireless card or USB11b wireless adapter following the instructions supplied with the card or adapter.

Wired Ethernet LAN

Each computer on the 10/100Base-T Ethernet LAN requires an Ethernet network interface card (NIC) and driver software installed. Because the SBG900 Ethernet port supports auto-MDIX, you can use straight-through or cross-over cable to connect a hub, switch, or computer. Use category 5 cabling for all Ethernet connections.

The physical wiring arrangement has no connection to the logical network allocation of IP addresses.

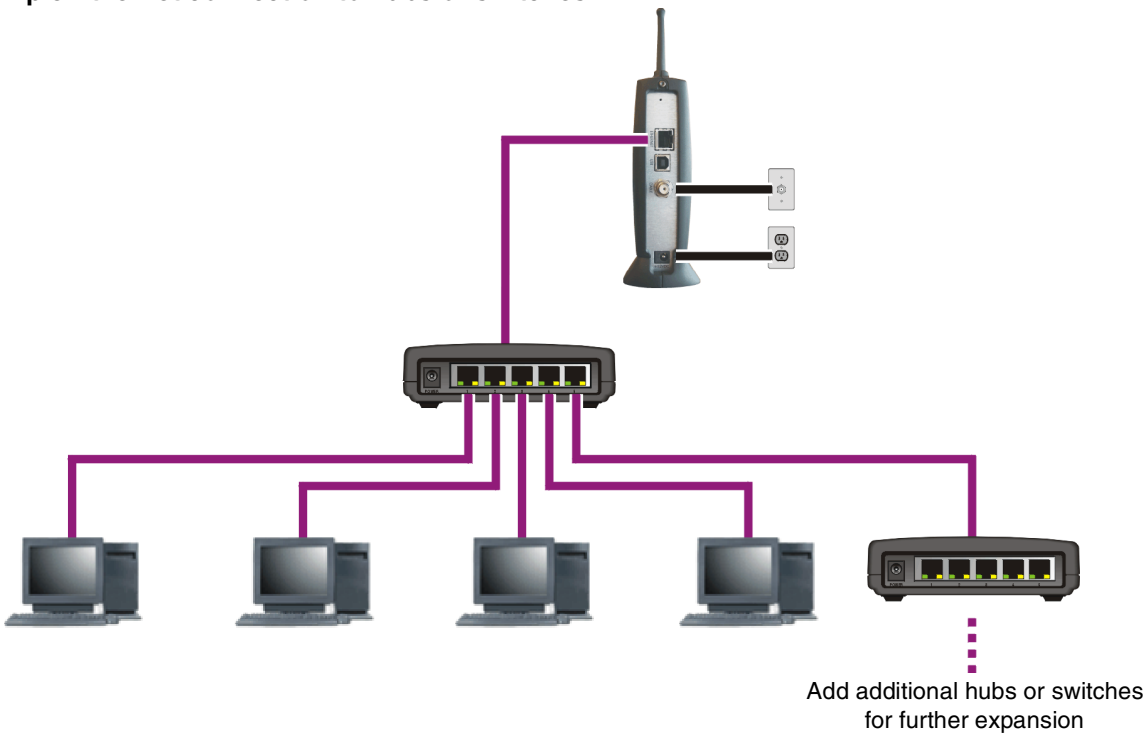
Sample Ethernet to computer connection



A wired Ethernet LAN with more than one computer requires one or more hubs or switches. You can connect a hub or switch to the Ethernet port on the SBG900.

The following illustration is an example of an Ethernet LAN you can set up using the SBG900. Cable the LAN in an appropriate manner for the site. A complete discussion of Ethernet cabling is beyond the scope of this document.

Sample Ethernet connection to hubs or switches



USB Connection

You can connect a single PC running Windows® 98, Windows XP™, Windows Me®, or Windows® 2000 to the SBG900 USB V1.1 port. For cabling instructions, see "Connecting a PC to the USB Port".

Caution!

Before plugging in the USB cable, be sure the Motorola SURFboard Wireless Cable Modem Gateway CD-ROM is inserted in the PC CD-ROM drive.

Sample USB connection

Security

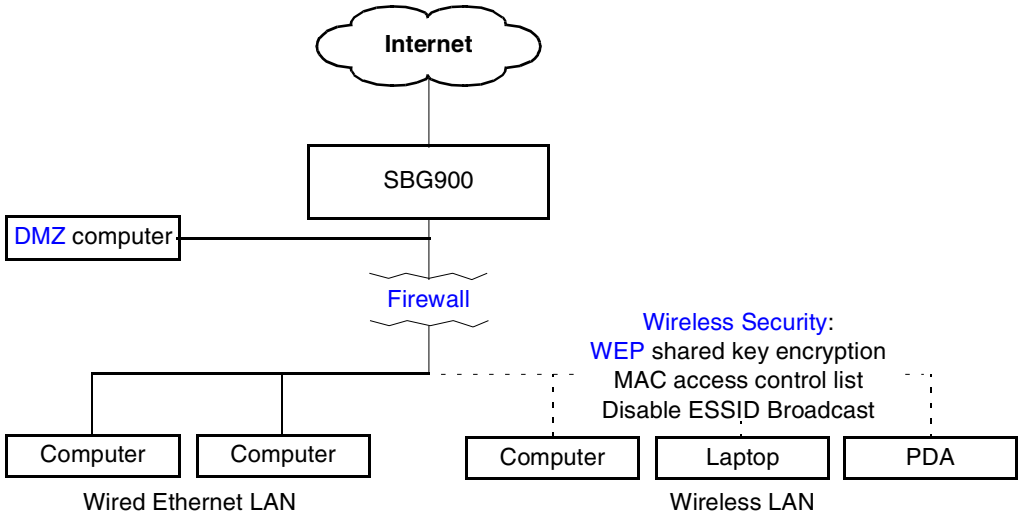
The SBG900 provides:

- A firewall to protect the SBG900 LAN from undesired attacks over the Internet
- Security measures to prevent eavesdropping of wireless data

Network Address Translation (NAT) provides some security because the IP addresses of SBG900 LAN computers are not visible on the Internet.

The logical network diagram does not necessarily correspond to the network cabling. A full discussion of network security is beyond the scope of this document.

SBG900 security measures shown in a logical network diagram



Firewall

The SBG900 firewall protects the SBG900 LAN from undesired attacks and other intrusions from the Internet. It provides an advanced integrated stateful-inspection firewall supporting intrusion detection, session tracking, and denial-of-service attack prevention. The firewall:

- Maintains state data for every TCP/IP session on the OSI network and transport layers
- Monitors all incoming and outgoing packets, applies the firewall policy to each one, and screens for improper packets and intrusion attempts
- Provides comprehensive logging for all:
  - User authentications
  - Rejected internal and external connection requests
  - Session creation and termination
  - Outside attacks (intrusion detection)

You can configure the firewall filters to set rules for port usage. For information about choosing a predefined firewall policy template, see “Setting the Firewall Policy”.

DMZ

A de-militarized zone (DMZ) is one or more computers logically located outside the firewall between an SBG900 LAN and the Internet. A DMZ prevents direct access by outside users to private data.

For example, you can set up a web server on a DMZ computer to enable outside users to access your website without exposing confidential data on your network.

A DMZ can also be useful to play interactive games that may have a problem running through a firewall. You can leave a computer used for gaming *only* exposed to the Internet while protecting the rest of your network. For more information, see Gaming Configuration Guidelines.

Port Triggering

When you run a PC application that accesses the Internet, it typically initiates communications with a computer on the Internet. In some applications, especially gaming, the computer on the Internet also initiates communications with your PC. Because NAT does not normally allow these incoming connections to occur, the SBG900 supports port triggering.

The SBG900 is preconfigured with port triggering for common applications. You can also configure additional port triggers if needed on the Gateway > PORT TRIGGERS — custom Page.

Wireless Security

Because wireless LAN signals are transmitted using radio signals, it may be possible for your neighbor or someone else you do not want accessing your wireless LAN. You need to limit access to only the intended persons. To prevent unauthorized eavesdropping of data transmitted over the wireless LAN, you must enable wireless security. *The default SBG900 settings provide no security for transmitted data.*

The SBG900 enables you to use the following wireless security measures:

- Restrict access to computers having the same unique network name as the SBG900
- Encrypt data transmitted over the wireless interface by configuring a Wired Equivalency Privacy (WEP) key on the SBG900 and wireless LAN clients (stations)
- Define a MAC access control list to restrict wireless LAN access to clients based on the MAC address.

If you disable ESSID broadcasting to enable closed network operation, the SBG900 does not transmit the network name (ESSID). This provides additional protection because only wireless stations configured with your network name can communicate with the SBG900. Closed network operation is an enhancement of the IEEE 802.11b standard.

For information about configuring a wireless security, see “Setting Up the Wireless LAN”.

Port Forwarding

Port forwarding is the configuration of SBG logical data ports for applications having special network requirements.

The SBG900 opens logical data ports when a computer on its LAN sends data, such as e-mail messages or web data, to the Internet. A logical data port is different from a physical port, such as an Ethernet port. Data from a protocol must go through certain data ports. Here are the data ports used by some protocols:

Protocol	Port
FTP	20, 21
HTTP	80
NTP	123
Secure Shell	22
SMTP e-mail	25
Telnet	23

Some applications, such as games and videoconferencing, require multiple data ports. If you enable NAT, this can cause problems because NAT assumes that data sent through one port will return to the same port. You may need to configure port forwarding to run applications with special requirements.

To configure port forwarding, you must specify an inbound (source) port or range of ports. The inbound port opens only when data is sent to the inbound port and closes again after a specified time elapses with no data sent to it. You can configure up to 32 port forwarding entries using the Gateway > PORT FORWARDING — config Page.

Virtual Private Networks

The SBG900 allows multiple tunnel VPN pass-through operation to securely connect remote computers over the Internet through the SBG900. The SBG900:

- Is compatible with Point to Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP)
- Is fully interoperable with any IPSec client or gateway and ANX certified IPSec stacks

Related Documentation

The following documents also provide information you can use with the SBG900:

- *SURFboard Wireless Cable Modem Gateway Quick Start Guide*
- *PCC11b Wireless Card Quick Start Guide and on-line help on the PCC11b and USB11b Wireless Adapter CD-ROM*
- *USB11b Wireless Adapter Quick Start Guide and on-line help on the PCC11b and USB11b Wireless Adapter CD-ROM*

For the most recent documentation, visit the Product Documentation page on the Motorola Broadband website http://broadband.motorola.com.

Installation

The following subsections provide information about installing the SBG900 hardware:

- Before You Begin
- Precautions
- Signing Up for Service
- Computer System Requirements
- Connecting the SBG900 to the Cable System
- Cabling the LAN
- Obtaining an IP Address for Ethernet
- Connecting a PC to the USB Port

For information about wireless LAN setup, see "Setting Up the Wireless LAN".

Before You Begin

Before you begin the installation, check that you received the following items with your SBG900:

Item	Description
Power adapter cord	Connects the SBG 900 to the external AC power supply
10/100Base-T Ethernet cable	Connects to the Ethernet port
USB cable	Connects to the USB port
***Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM**	Contains this *User Guide* and USB drivers

You will need 75-ohm coaxial cable with F-type connectors to connect the SBG900 to the nearest cable outlet. If a TV is connected to the cable outlet, you may need a 5 to 900 MHz RF splitter and two additional coaxial cables to use both the TV and the SBG900.

Determine the connection types you will make to the SBG900. Check that you have the required cables, adapters, and adapter software. You may need:

Wireless LAN	Wireless adapter and driver software for each computer having a wireless connection (see "Optional Accessories")
Wired Ethernet LAN	Ethernet cables and network interface cards (NICs) with accompanying installation software To connect more than one computer to the SBG900, one or more Ethernet hubs or switches
USB	A USB cable and the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM containing the software for USB installation

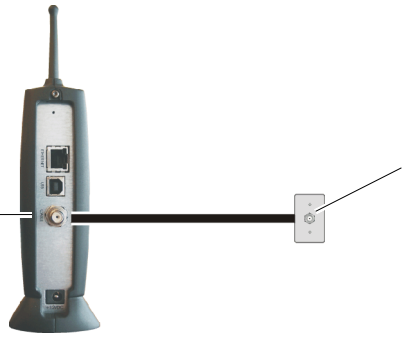
Coaxial cable, RF splitters, hubs, and switches are available at consumer electronic stores.

Precautions

Postpone SBG900 installation until there is no risk of thunderstorm or lightning activity in the area. SBG900.

To avoid damaging the SBG900 or computers with static electricity:

Before you connect or disconnect the USB or Ethernet cables, *always touch the coaxial cable connector on the* SBG900.



Always make the wall connection first.

- To avoid potential shock, always unplug the power cord from the wall outlet or other power source before disconnecting it from the SBG900 rear panel.
- To prevent overheating the SBG900, do not block the ventilation holes on the sides of the unit.
- Do not open the unit. Refer all service to your cable service provider.
- Wipe the unit with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the unit or use forced air to remove dust.

Signing Up for Service

You must sign up with a cable service provider to access the Internet and other online services.

To activate your service, call your local cable service provider.

You need to provide the MAC address marked **HFC MAC ID** printed on the Label on the Bottom of the SBG900. If you printed this document, you can record it here:

00 : _____ : _____ : _____ : _____ : _____

You should ask your cable service provider the following questions:

- Do you have any special system requirements?
- When can I begin to use my SBG900?
- Are there any files I need to download after I am connected?
- Do I need a user name or password to access the Internet or use e-mail?

Computer System Requirements

You can connect Microsoft Windows, Macintosh, UNIX, or Linux computers equipped as follows to the SBG900 LAN:

- *One* of the following:

  Ethernet 10Base-T or 10/100Base-T Ethernet adapter with proper NIC driver software installed

  Wireless Any IEEE 802.11g or IEEE 802.11b device
  For information about the Motorola PCC11b Wireless Card (PCMCIA type II 3.3 V slot) or USB11b Wireless Adapter, see “Optional Accessories”.

- PC with Pentium class or better processor
- Windows® 98, Windows® 98 SE, Windows Me®, Windows® 2000, Windows XP™, Windows NT®, Macintosh, or Linux operating system with operating system CD-ROM available
- Minimum 16 MB RAM recommended
- 10 MB available hard disk space

You can use any web browser such as Microsoft® Internet Explorer or Netscape Navigator® with the SBG900.

You can use the USB connection with any PC running Windows 98, Windows 2000, Windows Me, or Windows XP that has a USB interface. The USB connection requires special USB driver software that is supplied on the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM. You can upgrade your USB drivers from the Downloads page http://broadband.motorola.com/noflash/usb_drivers.asp on the Motorola Broadband website.

Connecting the SBG900 to the Cable System

1 Be sure the computer is on and the SBG900 is unplugged.

2 Connect one end of the coaxial cable to the cable outlet or splitter.

3 Connect the other end of the coaxial cable to the cable connector on the SBG900.

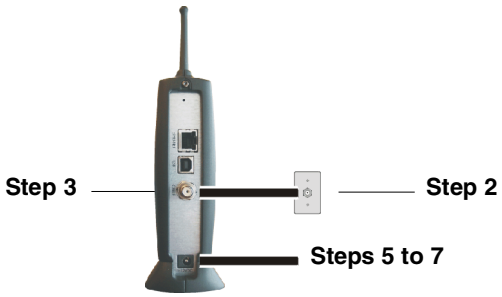
Hand-tighten the connectors to avoid damaging them.

4 Insert the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM into the CD-ROM drive.

5 Plug the power cord into the power connector on the SBG900.

6 Connect the external power supply.

7 Plug the power cord into the electrical outlet. *This turns the SBG900 on. You do not need to unplug it when not in use. The first time you plug in the SBG900, allow 5 to 30 minutes to find and lock on the appropriate communications channels.*



8 Check that the lights on the front panel cycle through this sequence:

POWER	Turns on when AC power is connected to the SBG900. Indicates that the power supply is working properly.
RECEIVE	Flashes while scanning for the receive channel. Changes to solid green when the receive channel is locked.
SEND	Flashes while scanning for the send channel. Changes to solid green when the send channel is locked.
ONLINE	Flashes during SBG900 registration and configuration. Changes to solid green when the SBG900 is registered.
PC/ACTIVITY	Flashes when the SBG900 is transmitting or receiving data.

Cabling the LAN

After connecting to the cable system, you can connect your wired Ethernet LAN. Some samples are shown in "Wired Ethernet LAN". On each networked computer, you must install proper drivers for the Ethernet NIC.

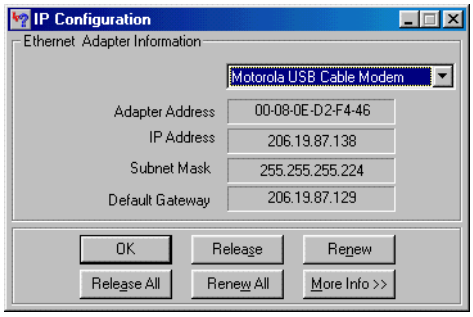
Detailed information about network cabling is beyond the scope of this document.

Obtaining an IP Address for Ethernet

Obtaining an IP Address in Windows 98, Windows 98 SE, or Windows Me

You must do the following on each Ethernet client PC running Windows 98, Windows 98 SE, or Windows Me:

1. On the Windows Desktop, click **Start**.
2. Select **Run**. The Run window is displayed.
3. Type **winipcfg.exe** and click **OK.** The IP Configuration window is displayed:



4. Click the **Renew** button to obtain an IP address for the PC from the DHCP server on the SBG900.

Obtaining an IP Address in Windows 2000 or Windows XP

You must do the following on each Ethernet client PC running Windows 2000 or Windows XP:

1. On the Windows Desktop, click **Start**.
2. Select **Run**. The Run window is displayed.
3. Type **cmd** and click **OK** to display a command prompt window.
4. Type **ipconfig /renew** and press **ENTER** to obtain an IP address for the PC from the DHCP server on the SBG900.
5. Type **exit** and press **ENTER** to return to Windows.

Obtaining an IP Address on Macintosh or UNIX Systems

Follow the instructions in your user manual.

Connecting a PC to the USB Port

You can connect a single PC running Windows 98, Windows XP, Windows Me, or Windows 2000 to the SBG900 USB port.

Caution!

Before plugging in the USB cable, be sure the Motorola SURFboard Wireless Cable Modem Gateway CD-ROM is inserted in the PC CD-ROM drive.

To connect a PC to the USB port:

1. Insert the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM in the CD-ROM drive.
2. Connect the USB cable to the USB port on the SBG900.
3. Connect the other end to the USB port on the computer.
4. Install the USB driver following the appropriate procedure for "Setting Up a USB Driver".

Basic Configuration

The following sections provide information about basic SBG900 configuration:

- Starting the SBG900 Setup Program
- Changing the Default Password
- Getting Help
- Setting the Firewall Policy
- Gaming Configuration Guidelines

For more advanced configuration information, see "Configuring TCP/IP", "Setting Up the Wireless LAN", or "Setting Up a USB Driver".

For normal operation, you do not need to change most default settings. The following caution statements summarize the issues you must be aware of:

Caution!

To prevent unauthorized configuration, change the default password *immediately* when you first configure the SBG900. See "Changing the Default Password".

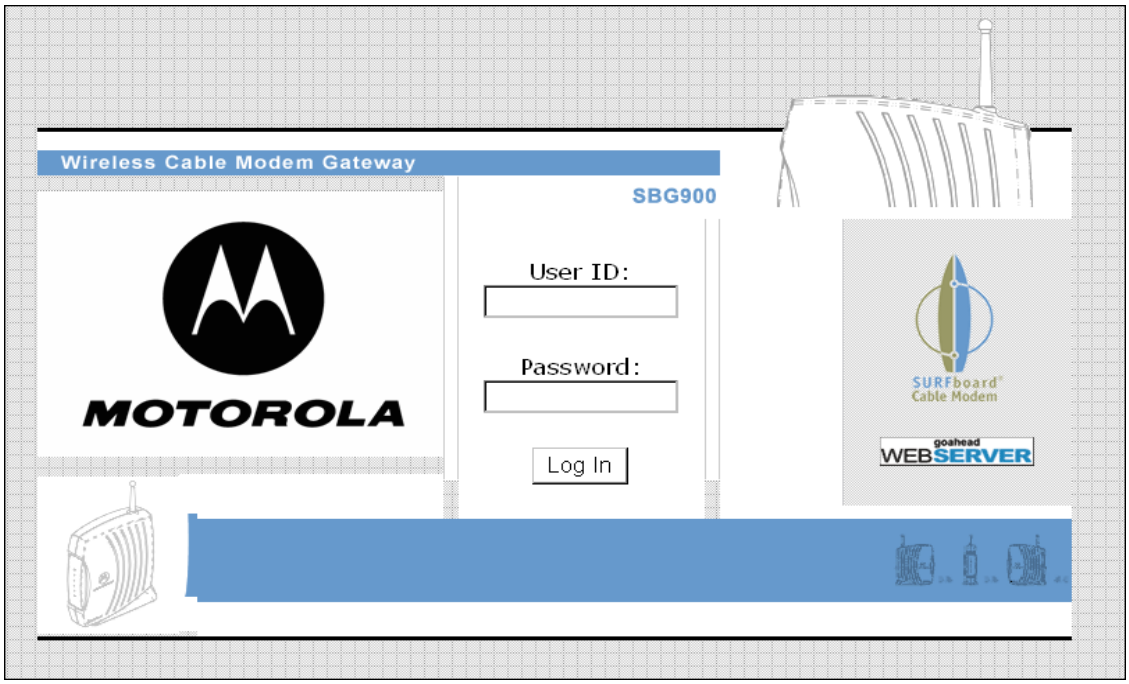
Firewalls are not foolproof. Choose the most secure firewall policy you can. See "Setting the Firewall Policy".

For a wireless LAN only, be sure you follow the instructions in "Setting Up the Wireless LAN".

Starting the SBG900 Setup Program

1 On a computer wired to the SBG900 over Ethernet or USB, open a web browser. *Do not attempt to configure the SBG900 over a wireless connection.*

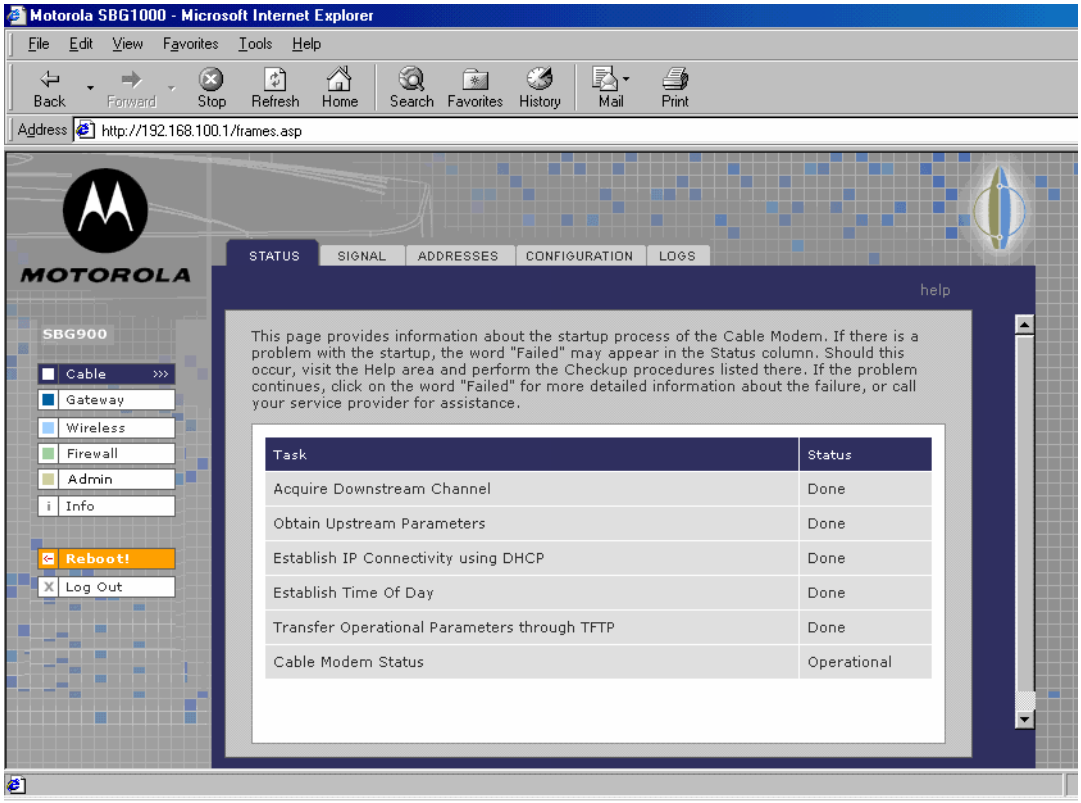
2 In the Address or Location field, type **http://192.168.100.1** and press **ENTER** to display the Login window:



3 In the **User ID** field, type the ***User Name***; the default is “admin” (this field is case sensitive).

4 In the **Password** field, type the ***Password***; the default is “motorola” (this field is case sensitive).

5 Click **Log In** to display the SBG900 user configuration and status windows:


Motorola SBG1000 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.100.1/frames.asp
MOTOROLA
STATUS SIGNAL ADDRESSES CONFIGURATION LOGS
help
SBG900
Cable
Gateway
Wireless
Firewall
Admin
Info
Reboot!
Log Out
This page provides information about the startup process of the Cable Modem. If there is a problem with the startup, the word "Failed" may appear in the Status column. Should this occur, visit the Help area and perform the Checkup procedures listed there. If the problem continues, click on the word "Failed" for more detailed information about the failure, or call your service provider for assistance.
Task
Status
Acquire Downstream Channel
Done
Obtain Upstream Parameters
Done
Establish IP Connectivity using DHCP
Done
Establish Time Of Day
Done
Transfer Operational Parameters through TFTP
Done
Cable Modem Status
Operational

Click	To Perform
Cable	Configure and monitor the cable system connection.
Gateway	Configure and monitor the gateway preferences (see Configuring the Gateway).
Wireless	Configure and monitor the wireless interface (see “Setting Up the Wireless LAN”).
Firewall	Configure and monitor the firewall (see “Setting the Firewall Policy”).
Admin	Changing the Default Password.
Info	Display information about the SBG900 Setup Program.
Reboot	Restart the SBG900. It is the same as pressing the reset button on the rear panel for less than five seconds.
Log Out	Log out of the SBG900.

If you have difficulty starting the SBG900 Setup Program, see “Troubleshooting” for information.

Router is a configuration option that may appear on your window but may not be supported.

For some settings, after you edit the field and click Apply, you are warned that you must reboot for your change to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log-in again.

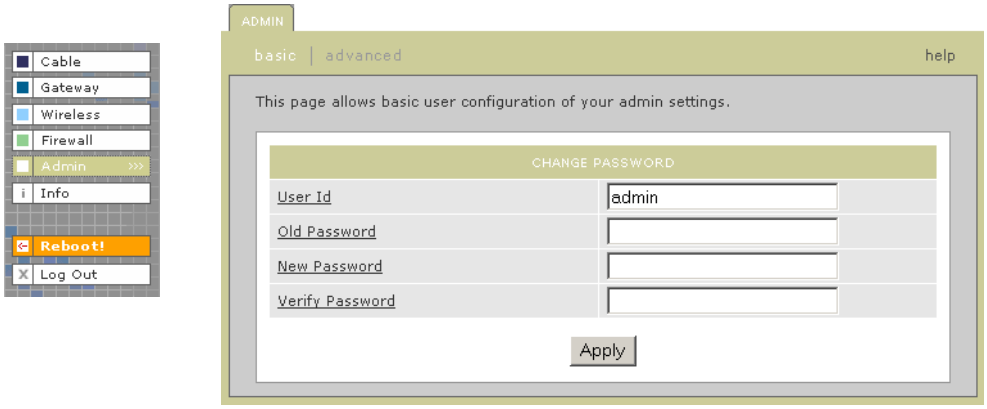
Changing the Default Password

Caution!

To prevent unauthorized configuration, change the default password *immediately* when you first configure the Motorola SURFboard Wireless Cable Modem Gateway.

To change the default password:

1 On the SBG900 Setup Program screen, click **Admin** to display the ADMIN — basic page:



2 In the **Old Password** field, type the old ***password***. The default password is “motorola” (this field is case sensitive).

3 In the **New Password** field, type the new ***password***.

4 In the **Verify Password** field, type the new ***password*** again.

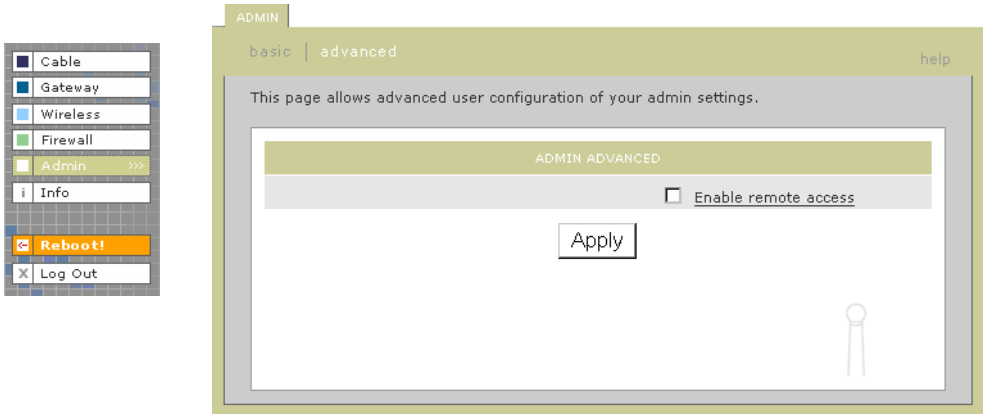
5 Click **Apply** to apply your changes.

Enabling Remote Access

Enabling remote access permits you to access the SBG900 from the Internet. You must know the **userid**, **password**, and **public IP address** assigned to your SBG900 to obtain access to the configuration pages from the Internet. Remote access is provided using a Web browser on the remote client, and connecting to the Web server on the SBG900.

To access the SBG900 remotely:

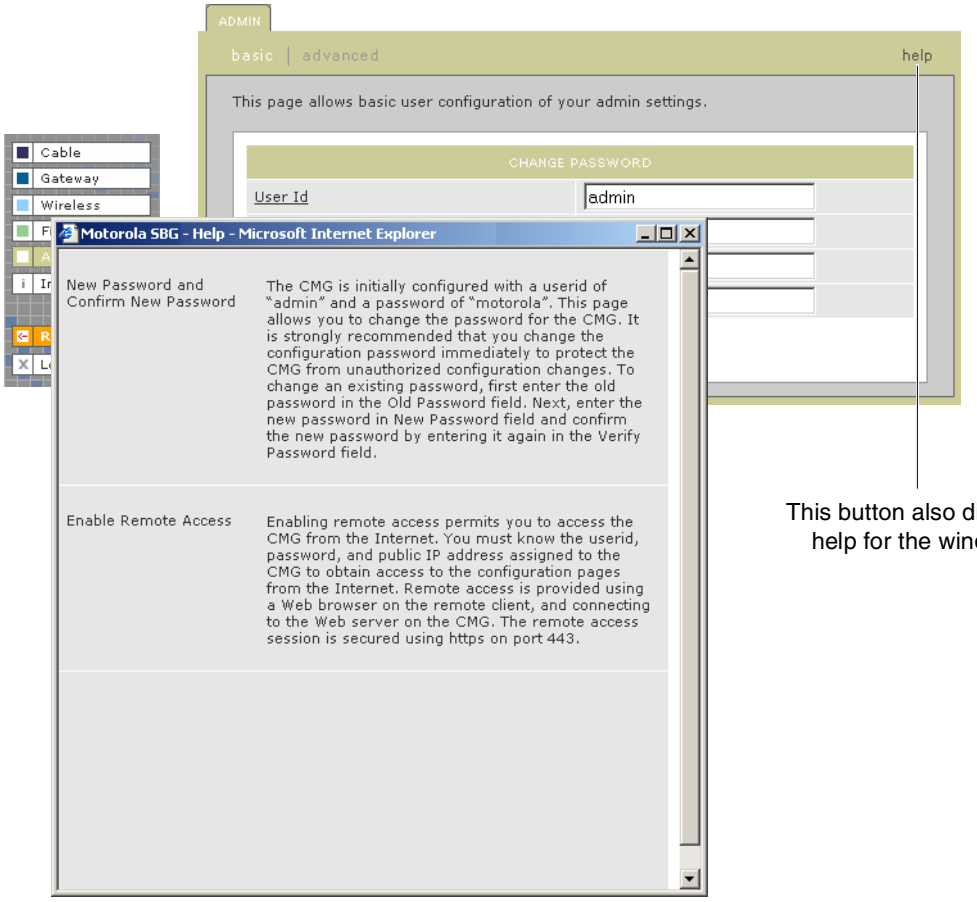
1. On the SBG900 Setup Program screen, click **Admin** to display the ADMIN — basic page.
2. Click **advanced** to display the ADMIN — advanced page.



3. Click the box next to **Enable remote access** to enable it.
4. Click **Apply** to apply your change.

Getting Help

To get help on any underlined item or field, click the text. For example, if you click a field or the help button on the ADMIN — basic page, the following help is displayed:


ADMIN
basic | advanced
help
This page allows basic user configuration of your admin settings.
CHANGE PASSWORD
User Id
admin
Cable
Gateway
Wireless
Motorola SBG - Help - Microsoft Internet Explorer
New Password and Confirm New Password
The CMG is initially configured with a userid of "admin" and a password of "motorola". This page allows you to change the password for the CMG. It is strongly recommended that you change the configuration password immediately to protect the CMG from unauthorized configuration changes. To change an existing password, first enter the old password in the Old Password field. Next, enter the new password in New Password field and confirm the new password by entering it again in the Verify Password field.
Enable Remote Access
Enabling remote access permits you to access the CMG from the Internet. You must know the userid, password, and public IP address assigned to the CMG to obtain access to the configuration pages from the Internet. Remote access is provided using a Web browser on the remote client, and connecting to the Web server on the CMG. The remote access session is secured using https on port 443.
This button also displays help for the window.

You can scroll to browse the help or click another item to display help for that item.

Setting the Firewall Policy

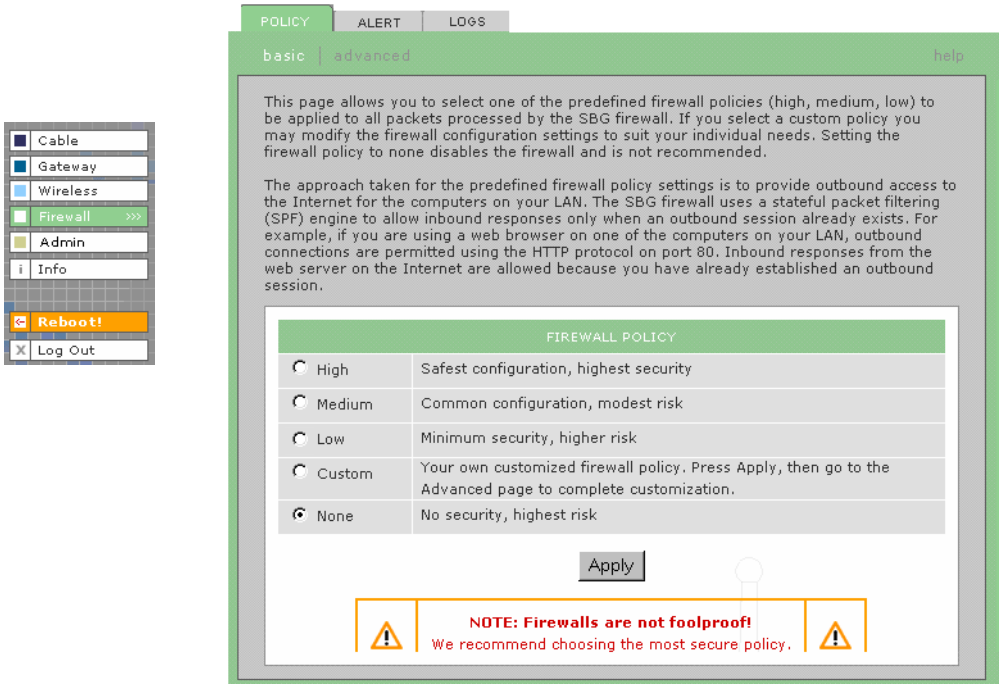
The SBG900 firewall protects the SBG900 LAN from undesired attacks and other intrusions from the Internet. This section describes using the Firewall > POLICY — basic page to choose one of the predefined firewall policy templates provided with the SBG900.

Caution!

Firewalls are not foolproof. Choose the most secure firewall policy you can. To enable easy network setup, the default firewall policy is None, which provides no security.

To select a predefined policy for all packets processed by the SBG900 firewall:

1. On the SBG900 Setup Program left panel, click **Firewall**.
2. Click **POLICY**.
3. Click **basic** to display the predefined firewall policy templates:


Cable
Gateway
Wireless
Firewall
Admin
Info
Reboot!
Log Out
POLICY
ALERT
LOGS
basic | advanced
help
This page allows you to select one of the predefined firewall policies (high, medium, low) to be applied to all packets processed by the SBG firewall. If you select a custom policy you may modify the firewall configuration settings to suit your individual needs. Setting the firewall policy to none disables the firewall and is not recommended.
The approach taken for the predefined firewall policy settings is to provide outbound access to the Internet for the computers on your LAN. The SBG firewall uses a stateful packet filtering (SPF) engine to allow inbound responses only when an outbound session already exists. For example, if you are using a web browser on one of the computers on your LAN, outbound connections are permitted using the HTTP protocol on port 80. Inbound responses from the web server on the Internet are allowed because you have already established an outbound session.
FIREWALL POLICY
High
Safest configuration, highest security
Medium
Common configuration, modest risk
Low
Minimum security, higher risk
Custom
Your own customized firewall policy. Press Apply, then go to the Advanced page to complete customization.
None
No security, highest risk
Apply
NOTE: Firewalls are not foolproof!
We recommend choosing the most secure policy.

4 Select the most secure firewall policy you can:

High The safest predefined firewall policy template, providing the highest security. *Motorola recommends this setting.*

Medium A predefined firewall policy template providing a common configuration having modest risk.

Low A predefined firewall policy template providing minimum security, with a higher risk of intrusions.

Custom You may need to create a custom firewall policy on the Firewall > POLICY — advanced Page. *Do not create a custom policy unless you have the necessary expertise and the need to do so.*

None Disables the firewall. To enable easy network setup, it is the default. *After you set up your network, use High, Medium, or Low to improve your security.*

5 Click **Apply** to apply your changes.

After you edit some fields and click Apply, you are warned that you must reboot for your change to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log-in again.

If you have the need, you can:

- View the rules for the High, Medium, or Low predefined policy templates or create a custom policy on the Firewall > POLICY — advanced Page
- Configure a firewall alert on Firewall > ALERT — basic Page and Firewall > ALERT — email Page
- View the firewall logs on the Firewall > LOGS Page

For information about how the firewall can affect gaming, see “Gaming Configuration Guidelines”.

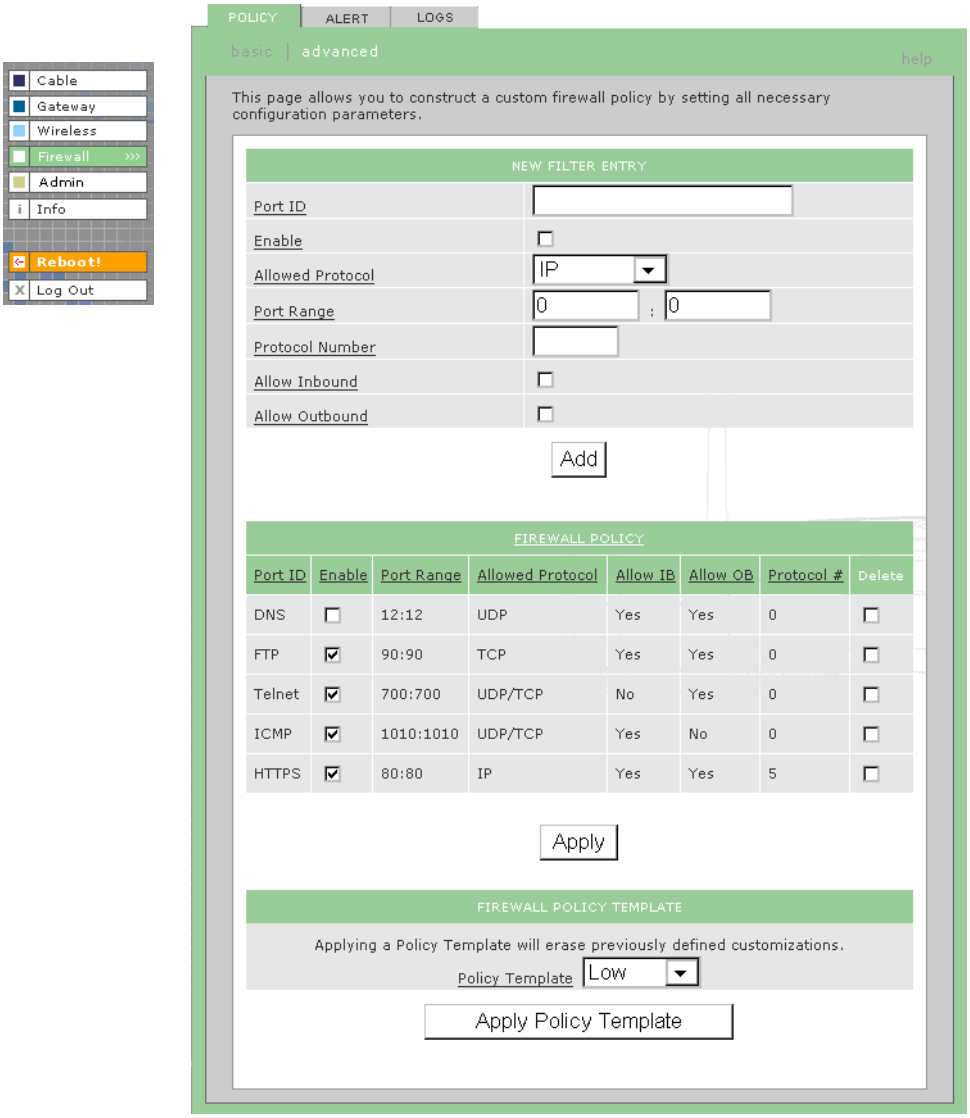
The predefined policies provide outbound Internet access for computers on the SBG900 LAN. The SBG900 firewall uses stateful inspection to allow inbound responses when there already is an outbound session running corresponding to the data flow. For example, if you use a web browser, outbound HTTP connections are permitted on port 80. Inbound responses from the Internet are allowed because an outbound session is established.

When required, you can configure the SBG900 firewall to allow inbound packets without first establishing an outbound session. You also need to configure a port forwarding entry on the Gateway > PORT FORWARDING — config Page or a DMZ client on the Gateway > LAN — nat config Page.

Firewall > POLICY — advanced Page

Do not create a custom firewall policy unless you have the necessary expertise and the need to do so. Instead, select one of the predefined policy templates as described in "Setting the Firewall Policy".

To create a custom firewall policy, first select **Custom** and click **Apply** on the Firewall > POLICY — basic Page. Then use this page to configure a custom firewall policy:



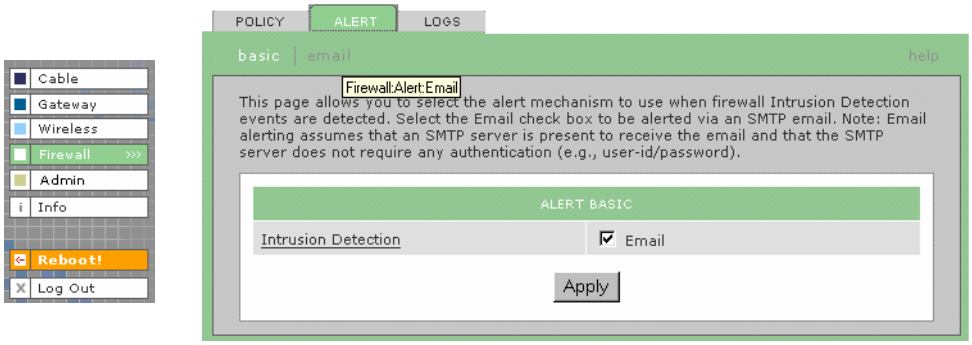
To base the custom policy on a predefined firewall policy template, choose High, Medium, or Low in the **Policy Template** field and click **Apply Policy Template**.

Firewall > POLICY — advanced page fields

Field	Description
NEW FILTER ENTRY	Section of the advanced policy window where you can construct a custom firewall
Port ID	The name of the protocol being filtered.
Enable	Check this box to enable firewall policy filtering for the port.
Allowed Protocol	The allowed protocols.
Port Range (From:To)	Sets the port range, which must contain all ports required by the protocol.
Protocol Number	The protocol number of the IP packets to allow.
Allow Inbound	Filters inbound data from the Internet on the specified ports.
Allow Outbound	Filters outbound data to the Internet on the specified ports. Stateful inspection ensures appropriate responses for outbound sessions.
Add	Click to add the new filter. It is displayed on the FIREWALL POLICY table.
FIREWALL POLICY Table	Lists the firewall policies.
Enable	Check this box to enable firewall policy filtering for the port.
Delete	Select the Delete box to delete the filter.
Apply	Click to apply your changes.
FIREWALL POLICY TEMPLATE	Enables you to select a predefined firewall policy template on which to base your custom template — High, Medium, or Low.
Apply Policy Template	Click to apply the selected predefined firewall policy template and cancel any customizations.

Firewall > ALERT — basic Page

You can use this page to set the alert mechanism for firewall intrusion detection events.

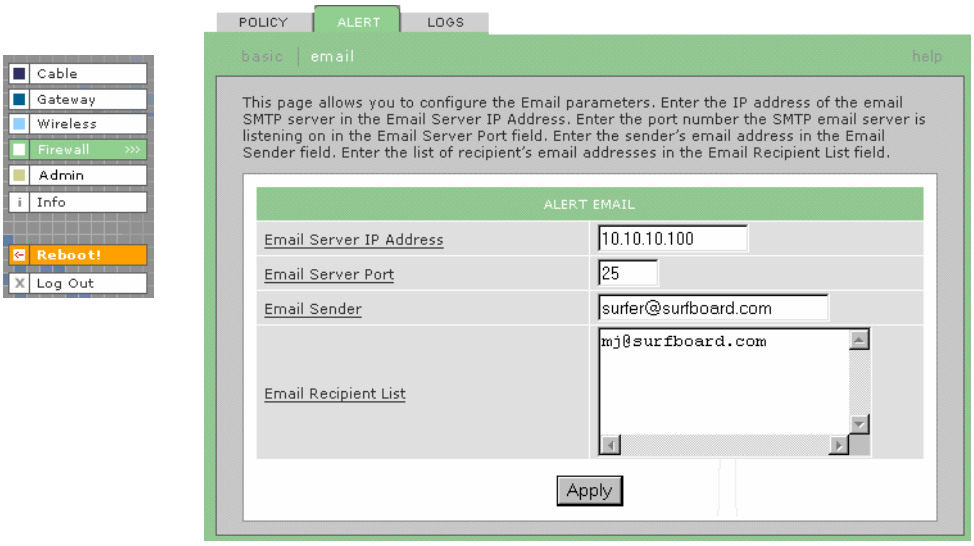

Cable
Gateway
Wireless
Firewall
Admin
Info
Reboot!
Log Out
POLICY
ALERT
LOGS
basic | email
help
Firewall:Alert:Email
This page allows you to select the alert mechanism to use when firewall Intrusion Detection events are detected. Select the Email check box to be alerted via an SMTP email. Note: Email alerting assumes that an SMTP server is present to receive the email and that the SMTP server does not require any authentication (e.g., user-id/password).
ALERT BASIC
Intrusion Detection
Email
Apply

Firewall > ALERT — basic page fields

Field or Button	Description
Intrusion Detection	Check Email to be alerted through SMTP e-mail. An SMTP server that does not require any authentication such as a user name or password must be present to receive the e-mail.
Apply	Click to apply your changes.

Firewall > ALERT — email Page

You can use this page to configure the e-mail alert parameters:

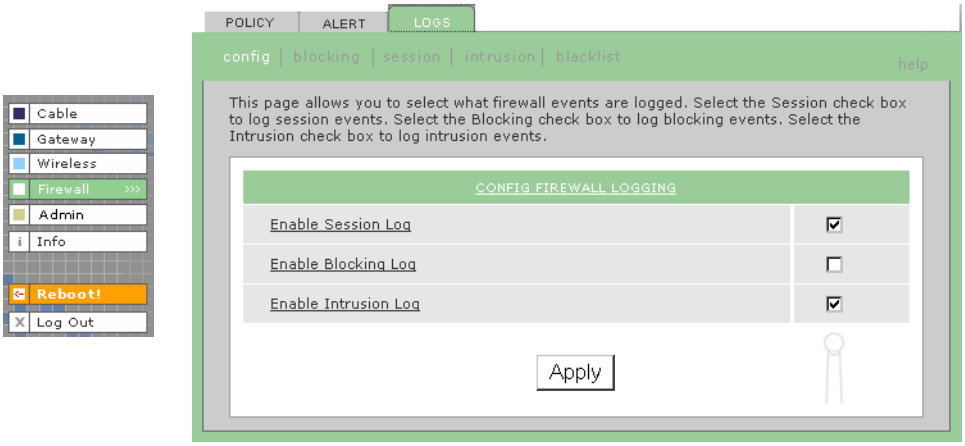

Cable
Gateway
Wireless
Firewall
Admin
Info
Reboot!
Log Out
POLICY
ALERT
LOGS
basic | email
help
This page allows you to configure the Email parameters. Enter the IP address of the email SMTP server in the Email Server IP Address. Enter the port number the SMTP email server is listening on in the Email Server Port field. Enter the sender's email address in the Email Sender field. Enter the list of recipient's email addresses in the Email Recipient List field.
ALERT EMAIL
Email Server IP Address
10.10.10.100
Email Server Port
25
Email Sender
surfer@surfboard.com
Email Recipient List
mj@surfboard.com
Apply

Firewall > ALERT — email page fields

Field or Button	Description
E-mail Server IP Address	Sets the e-mail server IP address in dotted-decimal format.
E-mail Server Port	Sets the e-mail server port number.
E-mail Sender	Sets the sender e-mail address.
E-mail Recipient List	Sets the list of e-mail addresses that receive alerts from the SBG900 firewall.
Apply	Click to apply your changes.

Firewall > LOGS Page

You can use this page to set which firewall events are logged.



Firewall > LOGS page fields

Field or Button	Description
Enable Session Log	Check this box to log session events.
Enable Blocking Log	Check this box to log blocking events.
Enable Intrusion Log	Check this box to log intrusions.
Apply	Click to apply your changes.

Firewall > LOGS

Option	Description
Session Log	The Session Log shows data sessions that have occurred and tracked by the Firewall. To enable logging of sessions, the Enable Session Log option must be selected in the Firewall Logs Config Page. A firewall policy must be in effect for session events to be generated. If the firewall policy is set to None then no new session entry will be generated. The log entries correspond to data sessions that have occurred in the device that are authorized by the normal firewall filters. Usually, this log shows the history of normal data traffic. Though a session may be terminated early by the firewall due to policy or session change, or if the session is later determined by the firewall to be an intrusion attack.
Blocking Log	The Blocking Log shows firewall blocking events. To enable logging of blocking events, the Enable Blocking Log option must be selected in the Firewall Logs Config Page. A firewall policy must be in effect for blocking events to be generated. If the firewall policy is set to None then no new blocking entry will be generated. The log entries correspond to firewall blocking events that occur when unauthorized inbound or outbound data packets are detected. Unauthorized data packets are those that use protocols and/or ports that are not explicitly allowed by the current firewall policy. In addition, data packets that are determined to be invalid due to session time-outs or reassembly time-outs are also blocked.
Intrusion Log	The Intrusion Log shows the intrusions attempts that have occurred and stopped by the firewall. To enable logging of intrusion events, the Enable Intrusion Log option must be selected in the Firewall Logs Config Page. A firewall policy must be in effect for intrusion events to be generated. If the firewall policy is set to None then no new intrusion entry will be generated. The log entries correspond to intrusion attacks that have been detected and stopped by the firewall. The firewall is capable of detecting several well-known intrusion tactics that is used to attack a network device. This log is a history of those intrusion events.
Blacklist	The Blacklist Log shows the IP addresses that have been determined by the firewall to have breached the firewall policy of the SBG. A firewall policy must be in effect for blacklist entries to be generated. If the firewall policy is set to None then no new blacklist entry will be generated. Once an IP address has been blacklisted, the firewall will block all traffic to and from that IP address for 24 hours or when the SBG is rebooted. The user can manually clear the blacklist by pressing the Clear button on the Blacklist Page. Clearing the blacklist table also allows normal traffic to flow between the SBG and the formerly blacklisted entries

Gaming Configuration Guidelines

The following subsections provide information about configuring the SBG900 firewall and DMZ for gaming.

Configuring the Firewall for Gaming

By default, the SBG900 firewall is disabled. If, as recommended, you enable the firewall, refer to the game's documentation to ensure that the necessary ports are open for use by that game.

The pre-defined SBG firewall policies affect X-Box Live™ as follows:

Low XBox Live data can pass through the firewall. No user action is required.

Medium or high To enable X-Box Live traffic to pass, you must configure:

- Choose Custom on the Firewall > POLICY — basic Page
- UDP 88:88 and UDP/TCP 3074:3074 on the Firewall > POLICY — advanced Page

Configuring Port Triggers

Because the SBG has pre-defined port triggers for games using any of the following applications, no user action is required to enable them:

- DirectX 7 and DirectX 8
- MSN Games by Zone.com
- Battle.net®

For a list of games supported by Battle.net, visit http://www.battle.net.

You may need to create custom port triggers to enable other games to operate properly. If you set custom port triggers and enable the firewall, you must customize the firewall to allow traffic through those ports. To create custom port triggers, use the Gateway > PORT TRIGGERS — custom Page.

Configuring a Gaming DMZ Host

Caution!

The gaming DMZ host is not protected by the firewall. It is open to communication or hacking from any computer on the Internet. Consider carefully before configuring a device to be in the DMZ.

Some games and game devices require *one* of:

- The use of random ports
- The forwarding of unsolicited traffic

For example, to connect a PlayStation® 2 for PS2® on-line gaming, designate it as the gaming DMZ host because the ports required vary from game to game. For these games, we recommend configuring the gaming computer or device as a gaming DMZ device.

To configure a gaming DMZ device, on the Gateway > LAN — dhcp leases Page:

1. Reserve a private IP address for the computer or game device MAC address.
2. Designate the device as a DMZ device.

You can reserve IP addresses for multiple devices, but only one can be designated as the gaming DMZ at once.

Configuring the Gateway

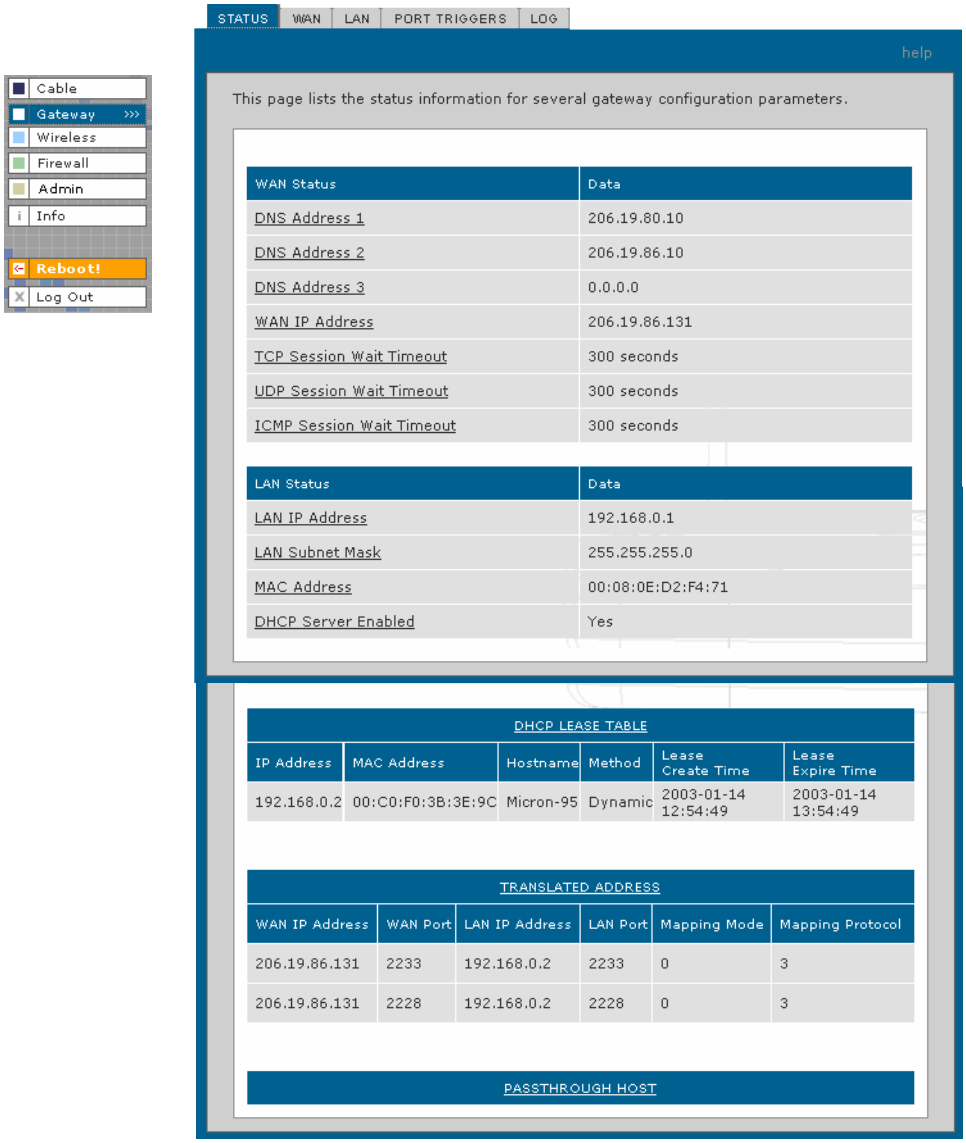
This section describes the Gateway configuration pages in the SBG900 Setup Program:

- Gateway > STATUS Page
- Gateway > WAN Page
- Gateway > LAN — nat config Page
- Gateway > LAN — dhcp server config Page
- Gateway > LAN — dhcp leases Page
- Gateway > PORT FORWARDING — status Page
- Gateway > PORT FORWARDING — config Page
- Gateway > PORT TRIGGERS — predefined Page
- Gateway > PORT TRIGGERS — custom Page
- Gateway > LOG Page

After you edit some fields and click Apply, you are warned that you must reboot for your change to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log-in again.

Gateway > STATUS Page

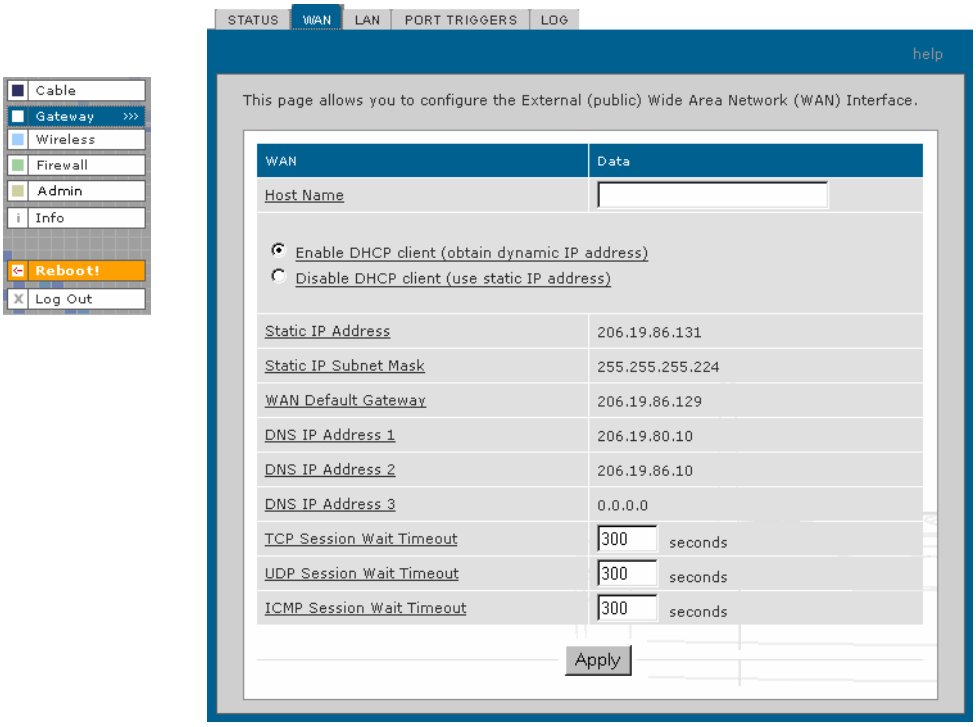
This page displays the gateway status information:



These fields display settings that are set on the other Gateway pages. For field descriptions, see the following subsections that describe the fields on each tab.

Gateway > WAN Page

Use this page to configure the external (public) wide area network (WAN) interface:



Gateway > WAN page fields

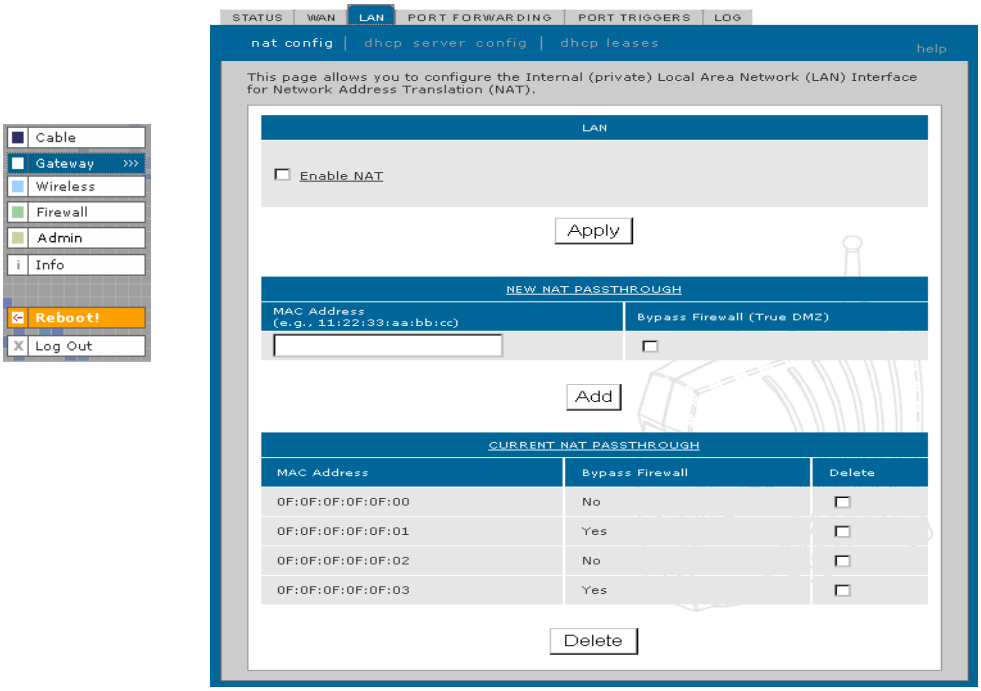
Field	Description
Host Name	If the cable service provider requires a hostname to access to their network, type the *hostname* they provided in this field. The default is None.
Enable DHCP Client	Enabling the DHCP client causes the wireless gateway to automatically obtain the public IP address, subnet mask, domain name, and DNS server(s). Most commonly, the DHCP client is enabled if the cable service provider automatically assigns a public IP address from their DHCP server. Enable DHCP Client is on by default.
Disable DHCP Client	If the cable service provider does not automatically assign a public IP address using DHCP, they must provide a static IP address. Select Disable DHCP Client. When you disable the DHCP client, you must type the static IP address, subnet mask, DNS server(s), and domain name (if necessary) in the fields provided. Disable DHCP Client is off by default.
Static IP Address	If Disable DHCP Client is on, type the static IP address provided by the cable service provider in dotted-decimal format. The default is None.
Static IP Subnet Mask	If Disable DHCP Client is on, type the subnet mask associated with the static IP address in dotted-decimal format. The default is None.
WAN Default Gateway	When using a statically assigned IP address from your ISP, enter the default gateway the SBG should be using to communicate with on the WAN.

Gateway > WAN page fields (continued)

Field	Description
DNS IP Address 1 **DNS IP Address 2** **DNS IP Address 3**	The cable service provider DNS server provides name-to-IP address resolution. If the cable service provider does not automatically assign DNS addresses from their DHCP server, they must provide at least one DNS server IP address to enter in these fields in dotted-decimal format. The default is None.
TCP Session Wait Timeout	Sets the maximum time in seconds to wait before assuming a TCP session has timed out. The default is 24 hours.
UDP Session Wait Timeout	Sets the maximum time in seconds to wait before assuming a UDP session has timed out. The default is 300 seconds (5 minutes).
ICMP Session Wait Timeout	Sets the maximum time in seconds to wait before assuming an ICMP session has timed out. The default is 300 seconds (5 minutes).
Apply	Click to apply your changes.

Gateway > LAN — nat config Page

Use this page to enable NAT and add clients to the CURRENT NAT PASSTHROUGH list:

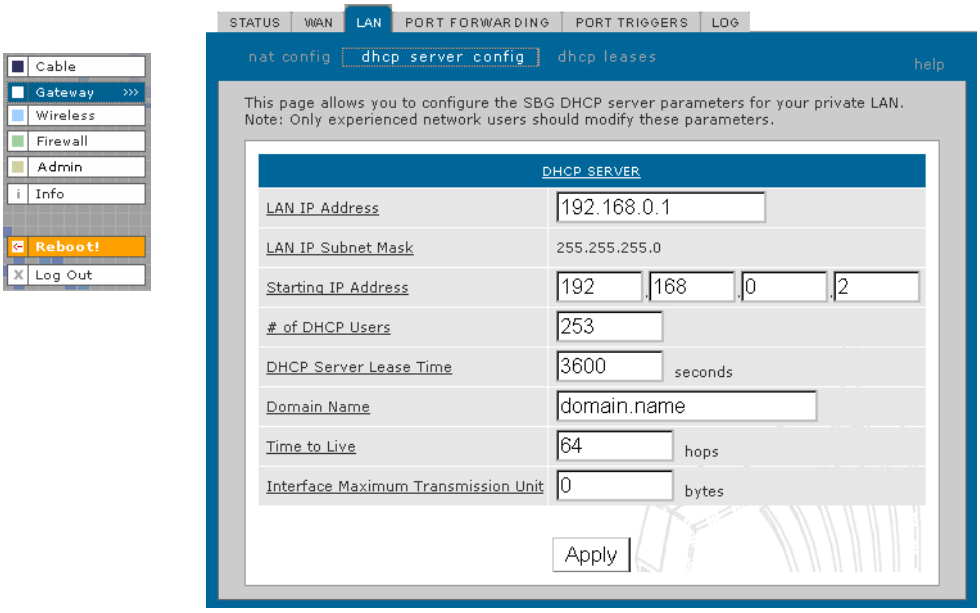


Gateway > LAN — nat config page fields

Field or Button	Description
LAN	
Enable NAT	If enabled, the single HFC IP Address (public IP address) assigned by the cable service provider is mapped to many private IP addresses on the SBG900 LAN.
Apply	Click to apply your changes. You must reboot the SBG900.
NEW NAT PASSTHROUGH	Specifies up to 32 computers as passthrough clients not subject to NAT, using their MAC addresses.
MAC Address	Type the passthrough client MAC address. The format is 16 hexadecimal numerals.
Bypass Firewall (True DMZ)	Check this box to set the NAT passthrough computer as a DMZ client. *Use this setting with extreme caution because a DMZ client is completely open to Internet hackers.*
Add	Click to add the MAC address to the CURRENT NAT PASSTHROUGH list.
CURRENT NAT PASSTHROUGH	Lists the computers on the LAN that are configured for NAT passthrough.
Delete	Click to delete the selected MAC address from the NAT passthrough list.

Gateway > LAN — dhcp server config Page

Only experienced network administrators should use this page to perform advanced DHCP server configuration:



CAUTION!

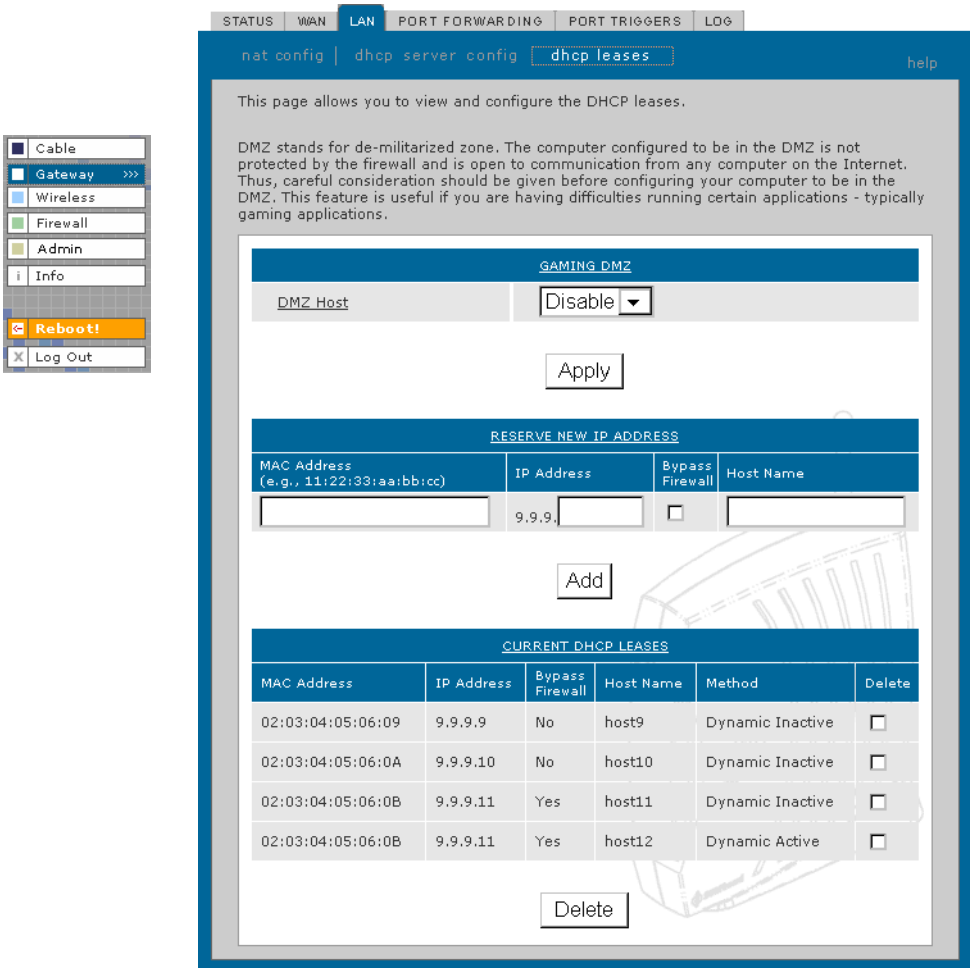
Do not modify these settings unless you are an experienced network administrator with strong knowledge of IP addressing, subnetting, and DHCP.

Gateway > LAN — dhcp server config page fields

Field	Description
LAN IP Address	Enter the IP address of the **SBG900** for your private LAN. The default is 192.168.0.1.
LAN IP Subnet Mask	The subnet mask in dotted-decimal format. The default is 255.255.255.0.
Starting IP Address	Enter the starting IP address to be assigned by the SBG900 DHCP server to clients in dotted-decimal format. The default is 192.168.0.2.
# of DHCP Users	Sets the number of clients for the SBG900 DHCP server to assign a private IP address. There are 253 possible client addresses. The default is 253.
DHCP Server Lease Time	Sets the time in seconds that the SBG900 DHCP server leases an IP address to a client. The default is 3600 seconds (60 minutes).
Domain Name	Sets the domain name for the SBG900 LAN. The default is None.
Time To Live	Sets the TTL (hop limit) for outbound packets. The default is 64.
Interface Maximum Transmission Unit	Sets the SBG900 LAN MTU in bytes. The minimum is 68 bytes. The default is 1500 bytes.
Apply	Click to apply your changes. You must reboot the SBG900.

Gateway > LAN — dhcp leases Page

Use this page to configure DHCP leases:



Gateway > LAN — dhcp leases page fields

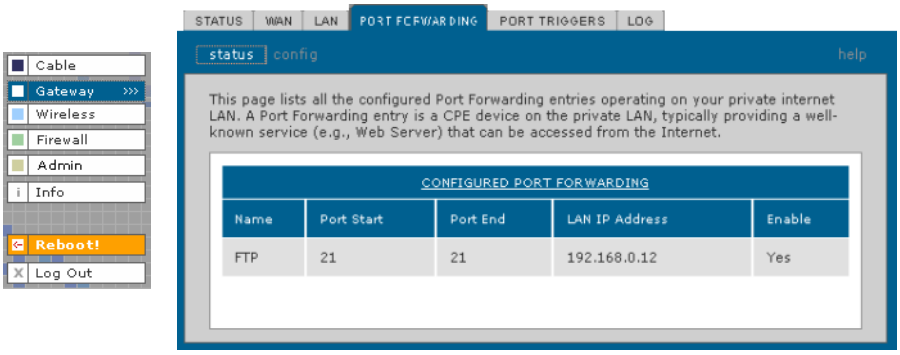
Field	Description
GAMING DMZ	
Enable Gaming DMZ	Check this box to designate the selected computer or gaming device as the gaming DMZ host. For more information, see "Configuring a Gaming DMZ Host". This can be useful if you have difficulties running certain applications; typically gaming applications.
(Gaming) DMZ Host	The gaming DMZ host is a computer with a reserved IP address designated as the default DMZ host. Only one gaming DMZ host can be active at once. *The gaming DMZ host is not protected by the firewall. It is open to communication or hacking from any computer on the Internet.* Consider carefully before configuring a computer to be in the DMZ. The benefit of using a gaming DMZ host instead of a NAT passthrough host is that a gaming DMZ host does not require a public IP address as does a NAT passthrough host. If the application requires a public IP address, configure the computer for NAT passthrough on the Gateway > LAN — nat config Page.

Gateway > LAN — dhcp leases page fields (continued)

Field	Description
RESERVE NEW IP ADDRESS	You can reserve up to 32 IP addresses assigned by the SBG900 DHCP server for specific LAN clients. For example, to ensure that they always receive the same private IP address, you can reserve IP addresses for a private FTP server or gaming DMZ device.
MAC Address	Type the MAC address of the DHCP client for which a reserved IP address is required. The format is 16 hexadecimal numerals.
IP Address	Sets the host portion of the reserved IP address for the LAN client having the specified MAC address. When the LAN client requests an IP address, the SBG900 DHCP server assigns the client this IP address.
Host Name	If your ISP requires a hostname to access their network, enter the hostname provided to you in the Host Name field.
Add	Click Add to reserve a new IP address.
CURRENTLY RESERVED IP ADDRESSES	Displays all DHCP clients having reserved IP addresses.
MAC Address	Displays the client MAC address.
IP Address	Displays its reserved IP address
Host Name	Displays its host name.
Method	Displays dynamic and static lease status. Add or delete dynamic or static lease status in this field.
Delete	Click this box to remove the reserved IP address for the client.
Delete	Click this button to remove the reserved IP addresses for clients designated by the Delete box.

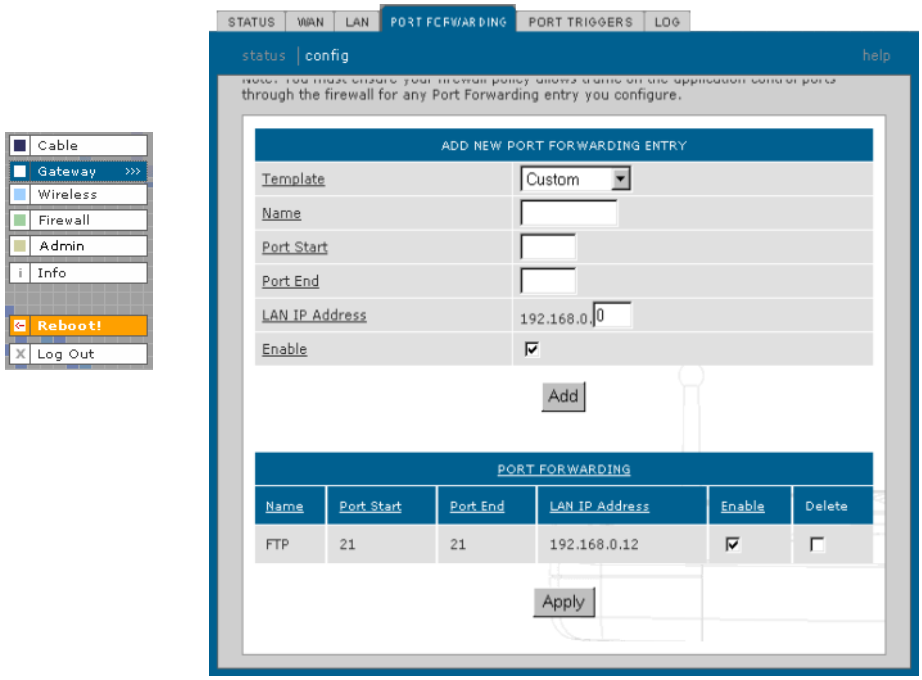
Gateway > PORT FORWARDING — status Page

Use this page to display the configured port forwarding entries on the SBG900 LAN. The fields are the same as on the Gateway > PORT FORWARDING — config Page:



Gateway > PORT FORWARDING — config Page

Use this page to configure up to 32 virtual servers:



Gateway > PORT FORWARDING — config page fields

Field	Description
ADD NEW PORT FORWARDING ENTRY	You can configure up to 32 virtual servers.
Template	If you select Custom, you must set the Name, Port Start, Port End, and LAN IP Address. If you select a predefined template such as HTTP or FTP, the Name, Port Start, Port End values are provided. You only need to enter LAN IP Address and change default values only if necessary.
Name	Type a unique identifier for the custom virtual server. The typical practice is to use the protocol as a unique identifier (for example “ftp”).
Port Start	Sets the LAN internal interface port or the start of a port range. Inbound Internet connection requests are statically mapped to this port.
Port End	If a range of ports is required, sets the end of the port range.
LAN IP Address	Sets the private LAN IP address for the port forwarding page. An Internet user must know the public IP address to access any port forwarding entry you define on the private LAN.
Enable	Check this box to enable the port forwarding entries to be accessed through NAT.
Add	Click to add the virtual server to the PORT FORWARDING list.
PORT FORWARDING	Displays the configured custom virtual servers.

Gateway > PORT TRIGGERS — predefined Page

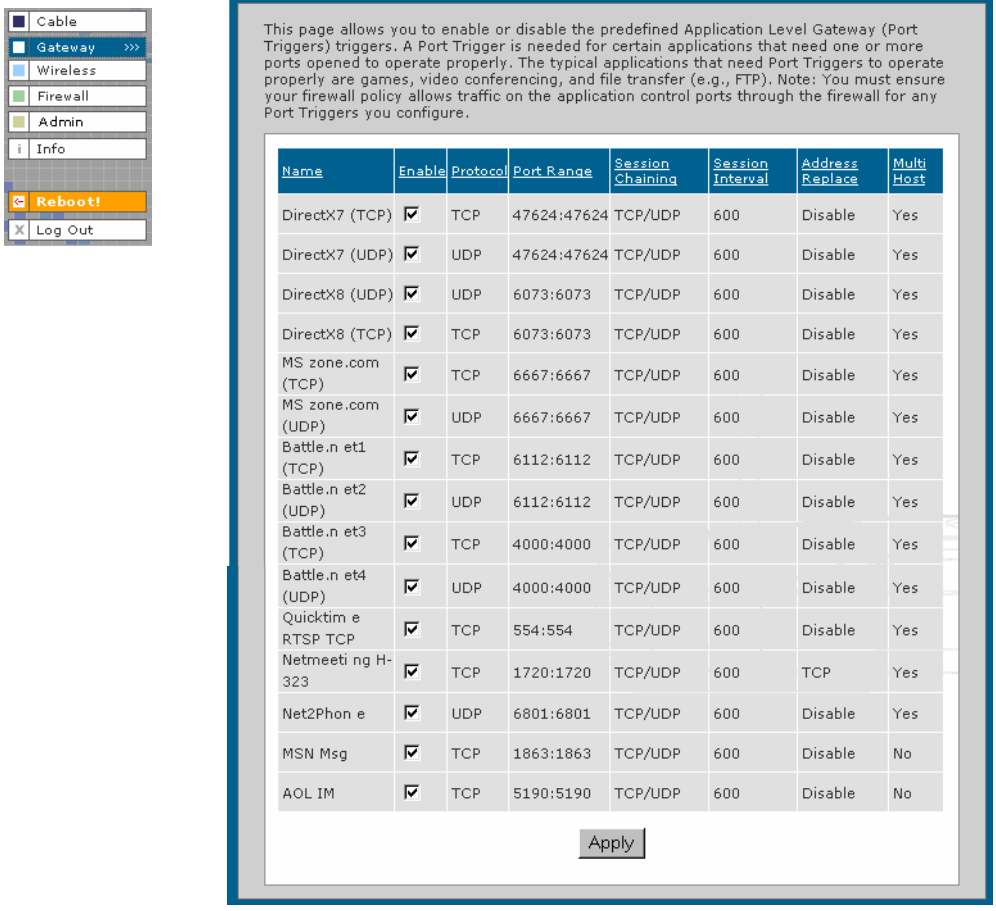
When you run a PC application that accesses the Internet, it communicates with a computer on the Internet. In some applications, especially gaming, the computer on the Internet also communicates with your PC. Because NAT does not normally allow these incoming connections, the SBG900 supports port triggering.

The SBG900 is preconfigured with port triggering for common applications. You can also configure additional port triggers if needed. Configuring port triggers for an application requires:

- The application transport protocol — TCP or UDP
- The application port number

You can use the default values for the remaining parameters.

Only one PC at a time connected to the SBG900 can use an application requiring port triggering. Use this page to view predefined port triggers:

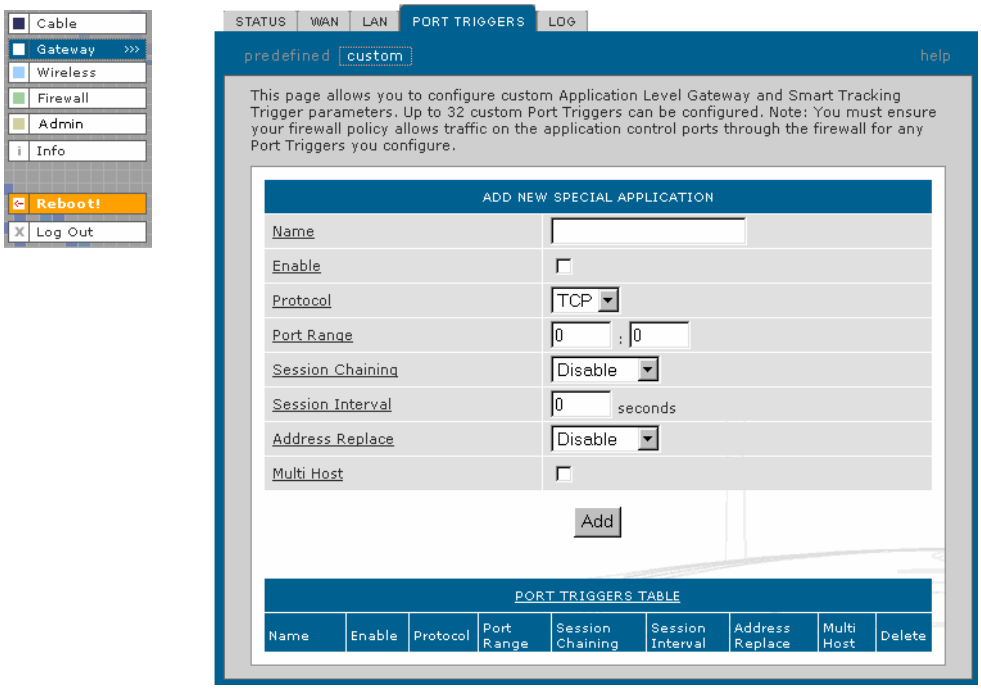

Cable
Gateway
Wireless
Firewall
Admin
Info
Reboot!
Log Out
STATUS
WAN
LAN
PORT TRIGGERS
LOG
predefined
custom
help
This page allows you to enable or disable the predefined Application Level Gateway (Port Triggers) triggers. A Port Trigger is needed for certain applications that need one or more ports opened to operate properly. The typical applications that need Port Triggers to operate properly are games, video conferencing, and file transfer (e.g., FTP). Note: You must ensure your firewall policy allows traffic on the application control ports through the firewall for any Port Triggers you configure.
Name
Enable
Protocol
Port Range
Session Chaining
Session Interval
Address Replace
Multi Host
DirectX7 (TCP) TCP 47624:47624 TCP/UDP 600 Disable Yes
DirectX7 (UDP) UDP 47624:47624 TCP/UDP 600 Disable Yes
DirectX8 (UDP) UDP 6073:6073 TCP/UDP 600 Disable Yes
DirectX8 (TCP) TCP 6073:6073 TCP/UDP 600 Disable Yes
MS zone.com (TCP) TCP 6667:6667 TCP/UDP 600 Disable Yes
MS zone.com (UDP) UDP 6667:6667 TCP/UDP 600 Disable Yes
Battle.n et1 (TCP) TCP 6112:6112 TCP/UDP 600 Disable Yes
Battle.n et2 (UDP) UDP 6112:6112 TCP/UDP 600 Disable Yes
Battle.n et3 (TCP) TCP 4000:4000 TCP/UDP 600 Disable Yes
Battle.n et4 (UDP) UDP 4000:4000 TCP/UDP 600 Disable Yes
Quicktim e RTSP TCP TCP 554:554 TCP/UDP 600 Disable Yes
Netmeeti ng H-323 TCP 1720:1720 TCP/UDP 600 TCP Yes
Net2Phon e UDP 6801:6801 TCP/UDP 600 Disable Yes
MSN Msg TCP 1863:1863 TCP/UDP 600 Disable No
AOL IM TCP 5190:5190 TCP/UDP 600 Disable No
Apply

Gateway > PORT TRIGGERS — predefined page fields

Field	Description
Name	Displays the unique name for the port triggers. This is typically the protocol name.
Enable	Select the Enable check box to activate the port triggers for the predefined application.
Protocol	Displays the transport protocol for the port trigger — TCP or UDP.
Port Range	Displays the port range (From/To) for the port trigger.
Session Chaining	Displays the session chaining selection for the port trigger — Disable, TCP, or TCP/UDP.
Session Interval	Displays the session interval set for the port trigger.
Address Replace	Displays the address replacement method for the port trigger.
Multi Host	Displays the multi host selection for the port trigger.

Gateway > PORT TRIGGERS — custom Page

Use this page to create a custom port trigger:



Gateway > PORT TRIGGERS — custom page fields

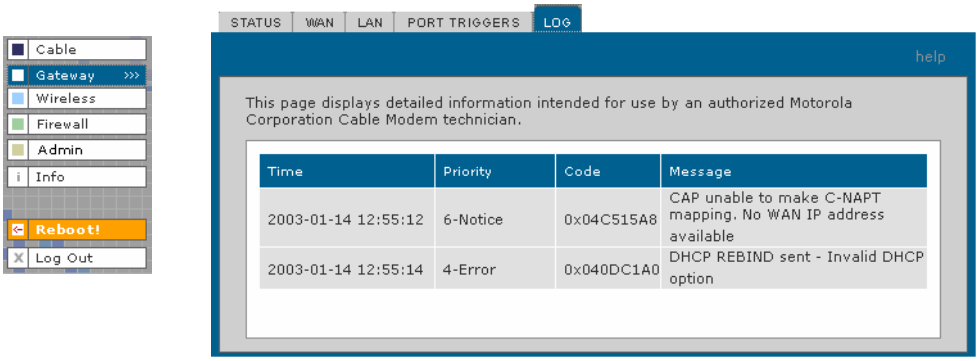
Field	Description
ADD NEW SPECIAL APPLICATION	
Name	Enter the unique name for the port trigger. This is typically the protocol.
Enable	Check this box to enable the custom port trigger.
Protocol	Sets the transport protocol for the port trigger — TCP or UDP.
Port Range (From:To)	Sets the port range for the port trigger. Type the start of the range in the left field and the end in the right field.
Session Chaining	Enable session chaining if the application needs to open one or more ports in different ranges to operate properly. The options are Disable, TCP, or TCP/UDP.
Session Interval	Sets the session interval for the application: • If the port triggers detect traffic on the Port Range within the Session Interval, it is considered to be related to the initial session. • If the port triggers detect traffic on the Port Range after the Session Interval expires, it is considered to be a new and unique session.
Address Replace	Sets the address replacement method for the application.
Multi Host	Check if appropriate for the application.
Add	Click to add the port trigger to the PORT TRIGGERS TABLE.

Gateway > PORT TRIGGERS — custom page fields

Field	Description
PORT TRIGGERS TABLE	Lists all port triggers you defined and their parameters.
Priority Port	Select the port to have a priority status.

Gateway > LOG Page

Use this page to view detailed information about the gateway:



Gateway > LOG page fields

Field	Description
Time	The date and time in the format yyyy-mm-dd hh:mm:ss (hours hh are 00 to 23).
Priority	Indicates the importance of the message.
Code	Code associated with this message.
Message	Describes the event.

Configuring TCP/IP

You must be sure all client computers are configured for TCP/IP (a protocol for communication between computers). Perform *one* of:

- Configuring TCP/IP in Windows 95, Windows 98, or Windows Me
- Configuring TCP/IP in Windows 2000
- Configuring TCP/IP in Windows XP
- Follow the instructions in your Macintosh or UNIX user manual

After configuring TCP/IP, perform *one* of the following to verify the IP address:

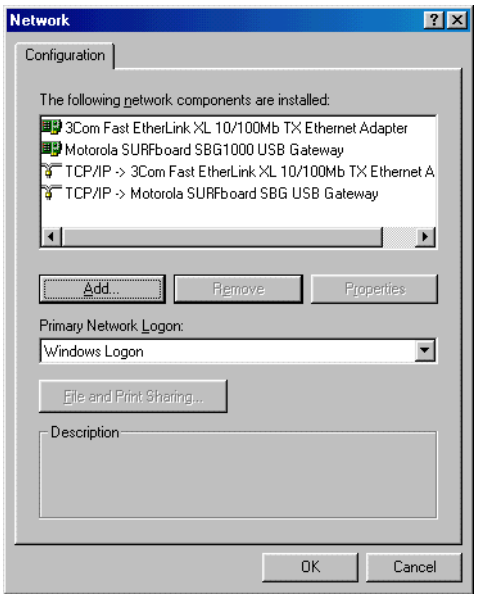
- Verifying the IP Address in Windows 95, Windows 98, or Windows Me
- Verifying the IP Address in Windows 2000 or Windows XP
- Follow the instructions in your Macintosh or UNIX user manual

Configuring TCP/IP in Windows 95, Windows 98, or Windows Me

1 On the Windows Desktop, click **Start**.

2 Select **Settings** and then **Control Panel** from the pop-up menus to display the Control Panel window.

3 Double-click the **Network** icon to display the Network window:

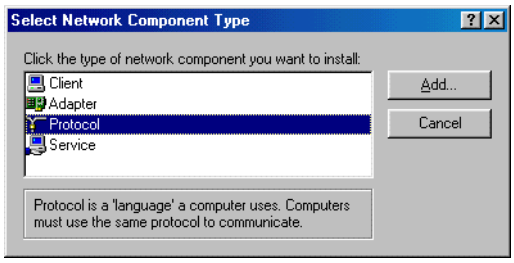


> Although your SBG model number may be different than in the images in this guide, the procedure is the same.

4 Select the **Configuration** tab.

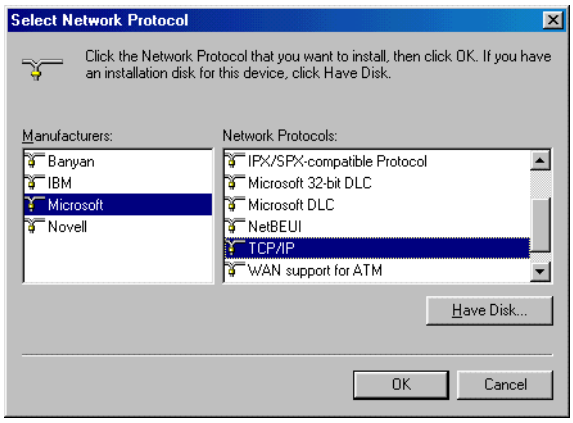
5 Verify that TCP/IP is installed for the adapter used to connect to the SBG900. If TCP/IP is installed, skip to step 10. If TCP/IP is not installed for the adapter, continue with step 6.

6 Select the adapter to use for the SBG900 connection and click **Add**. The Select Network Component Type window is displayed:



7 Click **Protocol** and click the **Add** button.

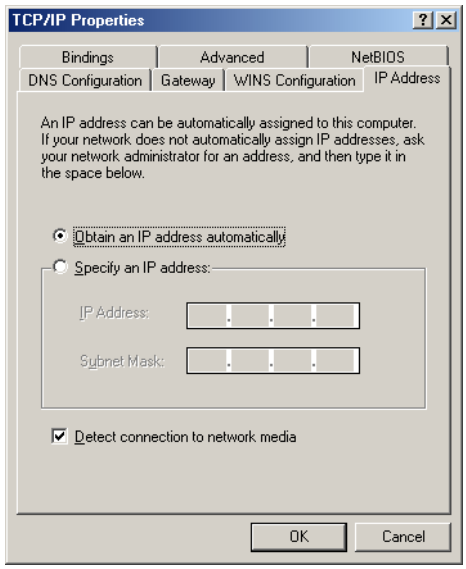
8 Click **Microsoft** in the Manufacturers section and click **TCP/IP** in the Network Protocol section of Select Network Protocol window:



9 Click **OK**.

10 Click **TCP/IP** on the Network window. If there is more than one TCP/IP entry, choose the one for the Ethernet card or USB port connected to the SBG900.

11 Click **Properties**. The TCP/IP Properties window is displayed:


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

12 Click the **IP Address** tab.

13 Click **Obtain an IP address automatically**.

14 Click **OK** to accept the TCP/IP settings.

15 Click **OK** to close the Network window.

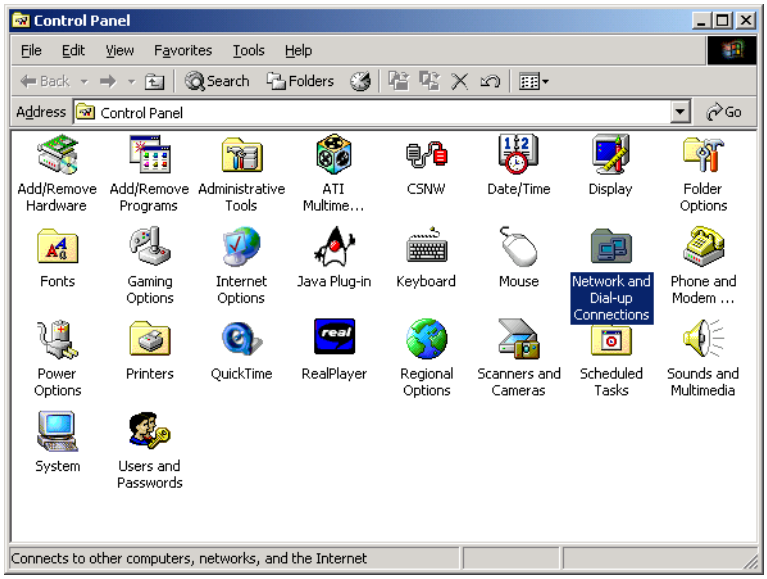
16 Click **OK** when prompted to restart the computer and click **OK** again.

When you complete TCP/IP configuration, go to "Verifying the IP Address in Windows 95, Windows 98, or Windows Me".

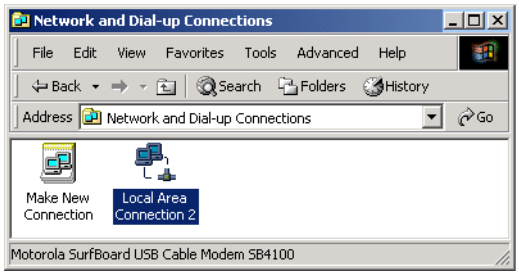
Configuring TCP/IP in Windows 2000

1 On the Windows Desktop, click **Start**.

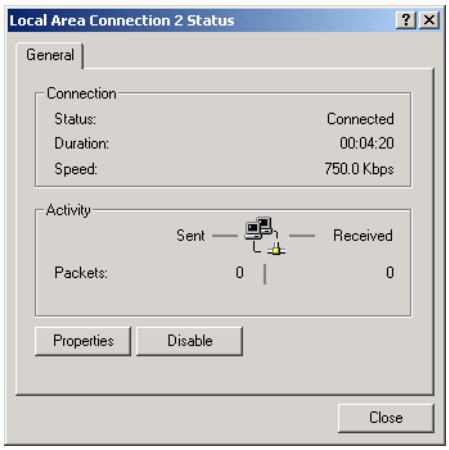
2 Select **Settings** and then **Control Panel** from the pop-up menus to display the Control Panel window:



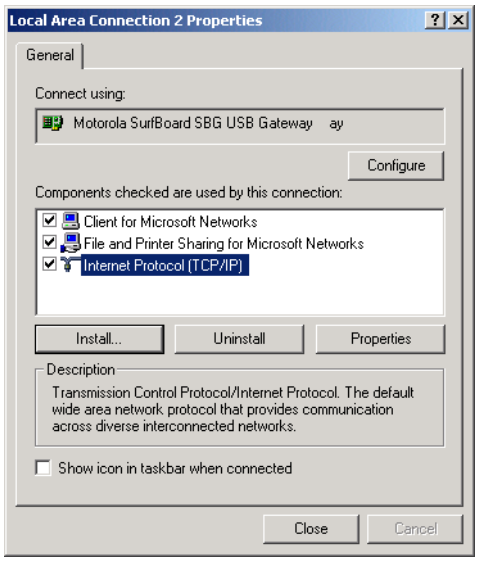
3 Double-click the **Network and Dial-up Connections** icon to display the Network and Dial-up Connections window:


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
Local Area Connection 2
Motorola SurfBoard USB Cable Modem SB4100

4 Click **Local Area Connection** *number*. The value of *number* varies from system to system. The Local Area Connection *number* Status window is displayed:

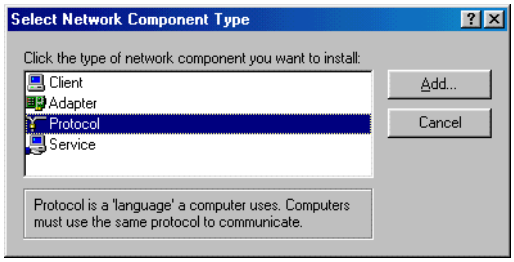


5 Click **Properties**. Information similar to the following window is displayed:

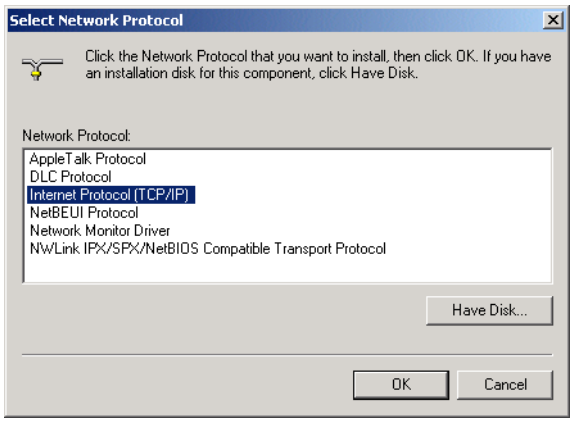


6 If Internet Protocol (TCP/IP) is in the list of components, TCP/IP is installed. You can skip to step 10.

If Internet Protocol (TCP/IP) is not in the list, click **Install**. The Select Network Component Type window is displayed:

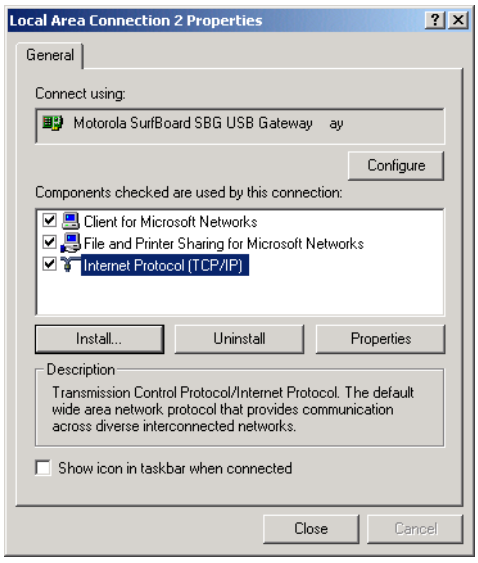


7 Click **Protocol** on the Select Network Component Type window and click **Add**. The Select Network Protocol window is displayed:


Select Network Protocol
Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.
Network Protocol:
AppleTalk Protocol
DLC Protocol
Internet Protocol (TCP/IP)
NetBEUI Protocol
Network Monitor Driver
NWLink IPX/SPX/NetBIOS Compatible Transport Protocol
Have Disk...
OK
Cancel

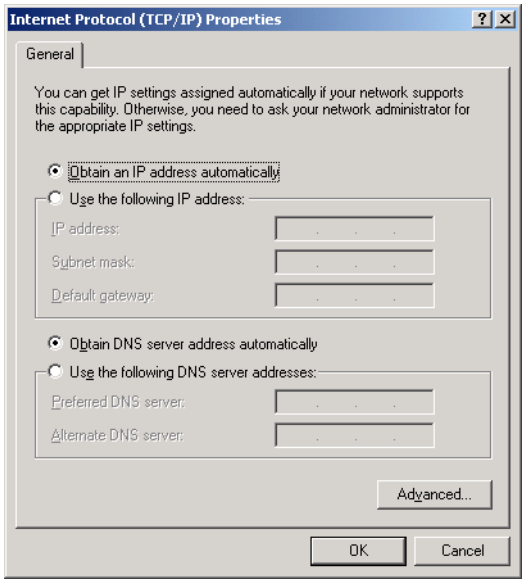
8 Click **Internet Protocol (TCP/IP)**.

9 Click **OK**. The Local Area Connection *number* Properties window is re-displayed.



10 Be sure the box next to Internet Protocol (TCP/IP) is checked.

11 Click **Properties**. The Internet Protocol (TCP/IP) Properties window is displayed:


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

12 Be sure **Obtain IP address automatically** and **Obtain DNS server address automatically** are selected.

13 Click **OK** to accept the TCP/IP settings.

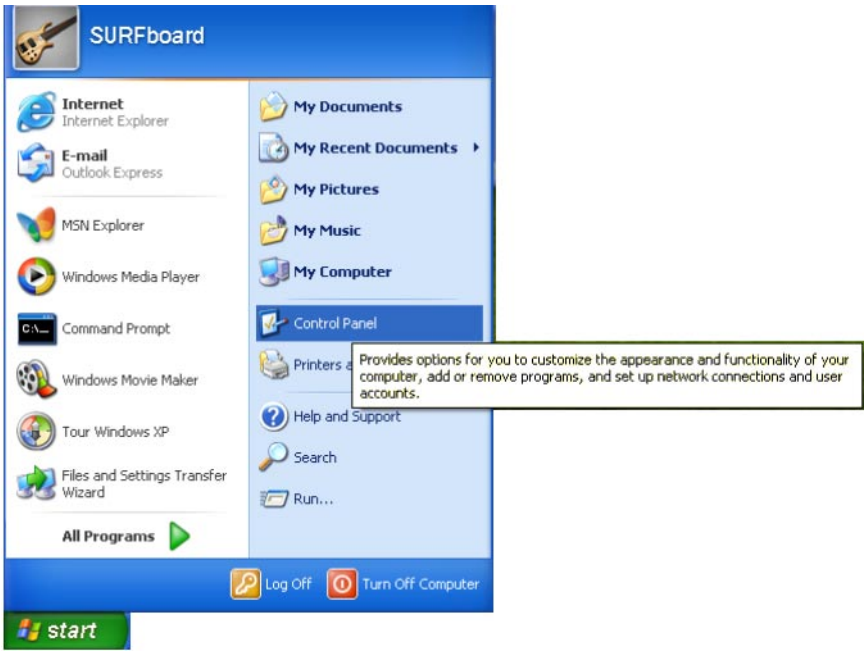
14 Click **OK** to close the Local Area Connection *number* Properties window.

15 Click **OK** when prompted to restart the computer and click **OK** again.

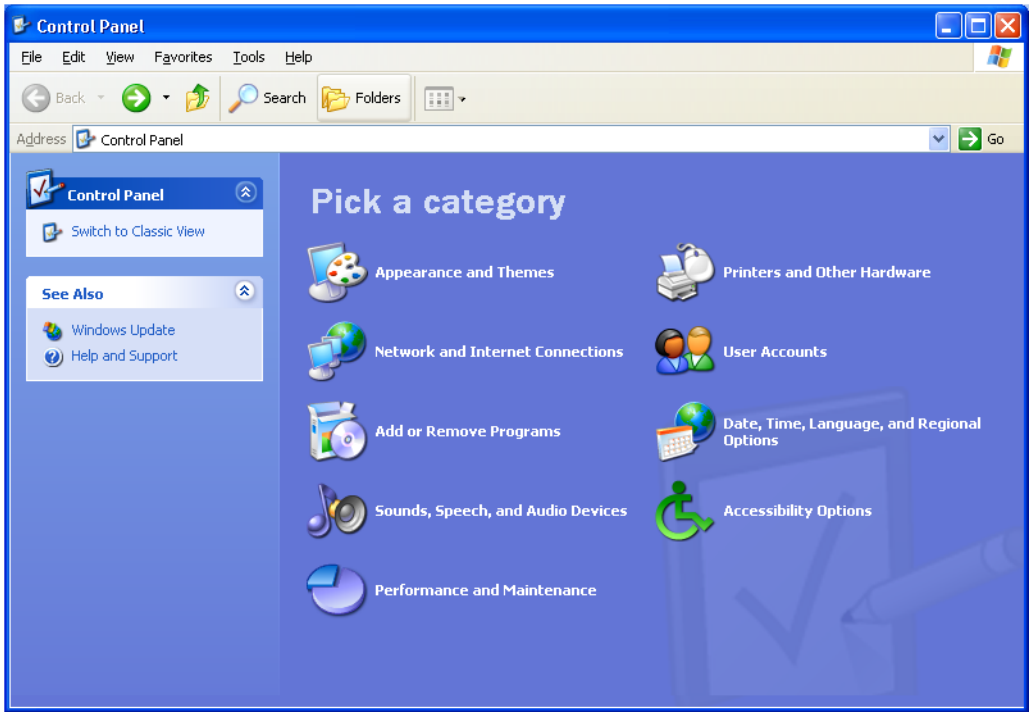
When you complete the TCP/IP configuration, go to "Verifying the IP Address in Windows 2000 or Windows XP".

Configuring TCP/IP in Windows XP

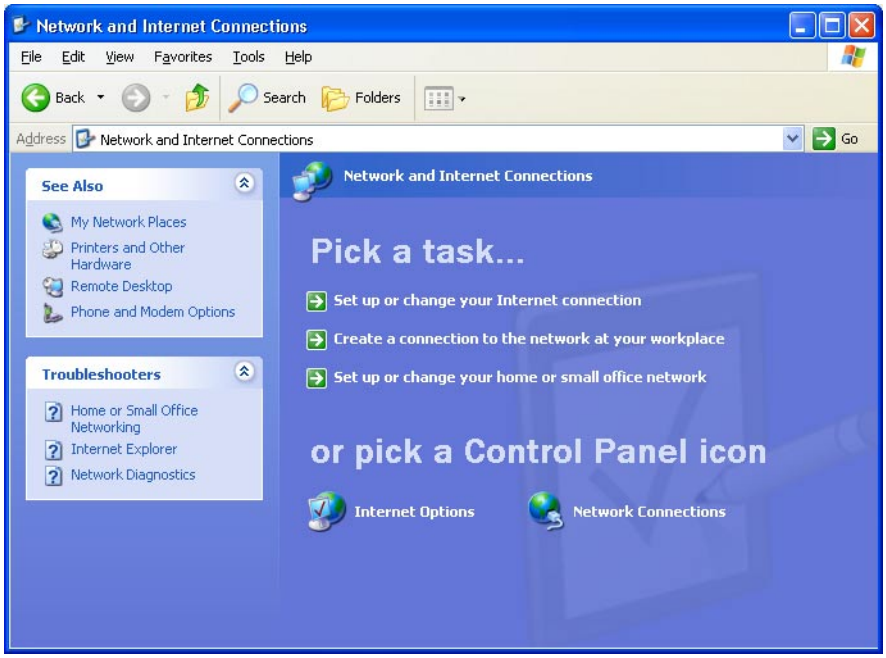
1 On the Windows desktop, click **Start** to display the Start window:



2 Click **Control Panel** to display the Control Panel window. The display varies, depending on the Windows XP view options. If the display is a Category view as shown below, continue with step 3. Otherwise, skip to step 5.

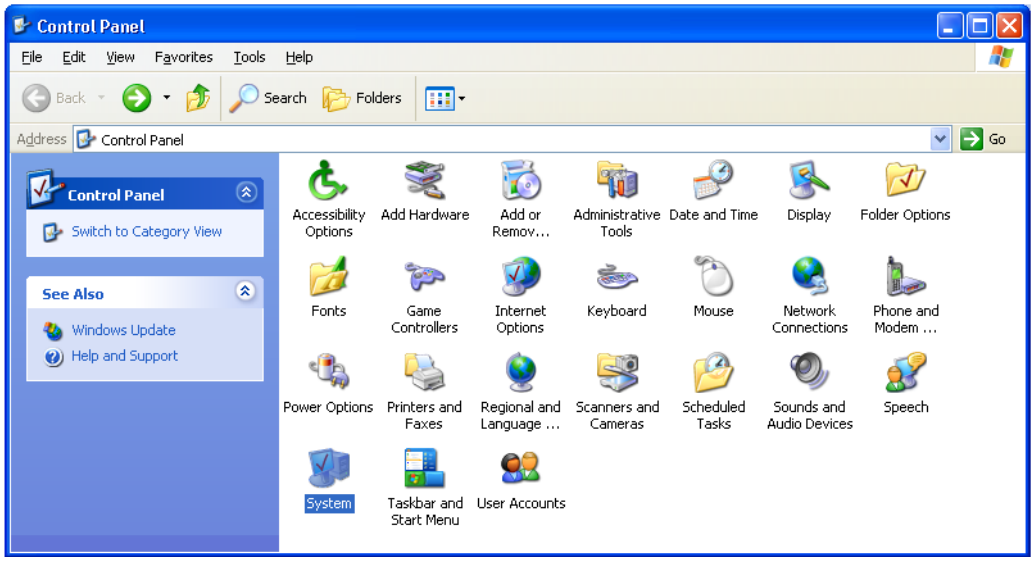


3 Click **Network and Internet Connections** to display the Network and Internet Connections window:


Network and Internet Connections
File Edit View Favorites Tools Help
Back Search Folders
Address Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
or pick a Control Panel icon
Internet Options
Network Connections

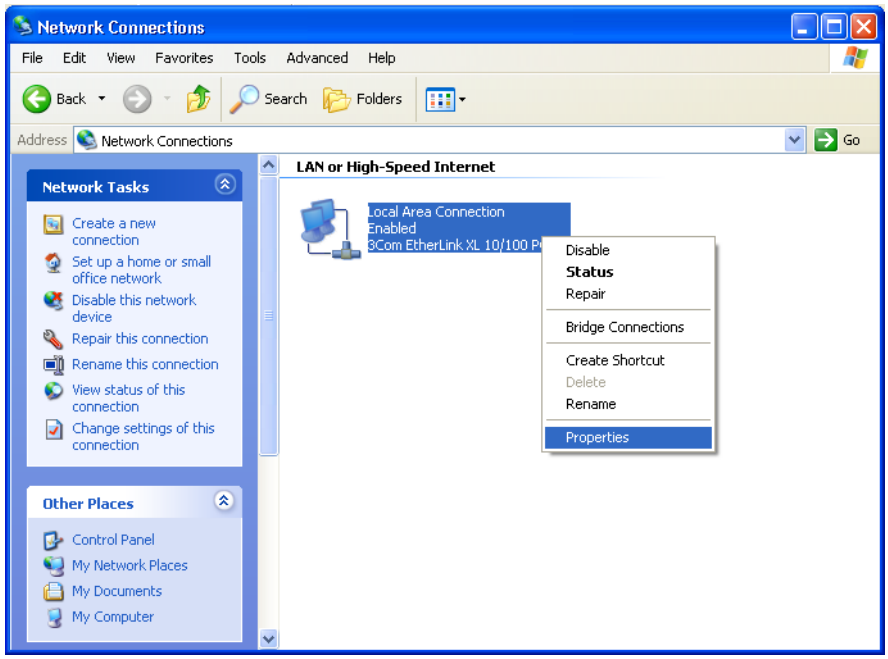
4 Click **Network Connections** to display the LAN or High-speed Internet connections. Skip to step 7.

5 If a classic view similar to below is displayed:

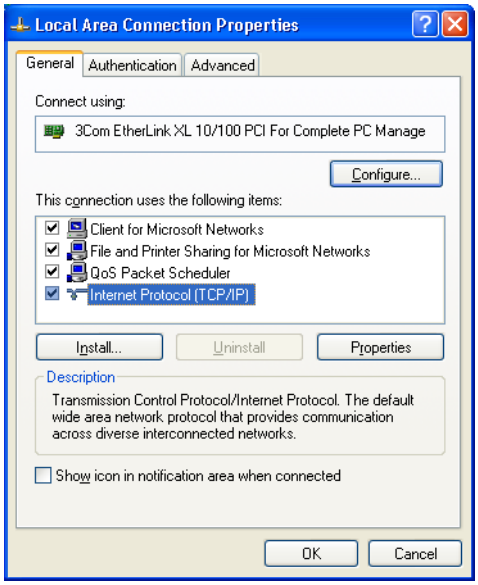


6 Click **Network Connections** to display the LAN or High-speed Internet connections.

7 Right-click on the network connection. If more than one connection is displayed, be sure to select the one for your network interface:

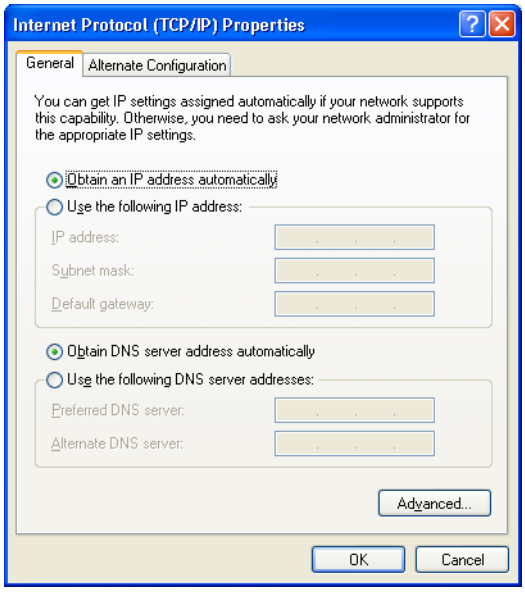


8 Select **Properties** from the pop-up menu to display the Local Area Connection Properties window:


Local Area Connection Properties
General Authentication Advanced
Connect using:
3Com EtherLink XL 10/100 PCI For Complete PC Manage
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

9 On the Local Area Connection Properties window, be sure Internet Protocol (TCP/IP) is checked. If it is not selected, check it.

10 Select **Internet Protocol (TCP/IP)** and click **Properties** to display the Internet Protocol (TCP/IP) Properties window:


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

11 Verify that the settings are correct, as shown above.

12 Click **OK** to close the TCP/IP Properties window.

13 Click **OK** to close the Local Area Connection Properties window.

When you complete the TCP/IP configuration, go to "Verifying the IP Address in Windows 2000 or Windows XP".

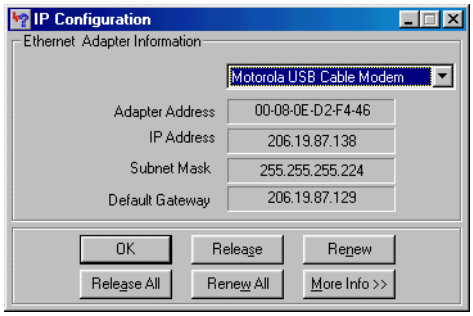
Verifying the IP Address in Windows 95, Windows 98, or Windows Me

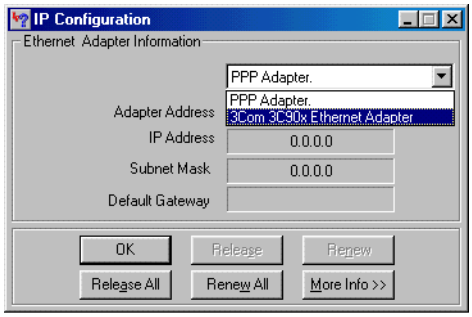
To check the IP address:

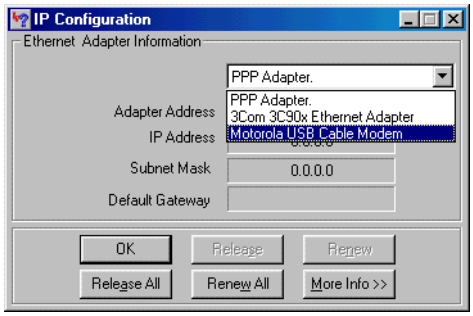
1 On the Windows Desktop, click **Start**.

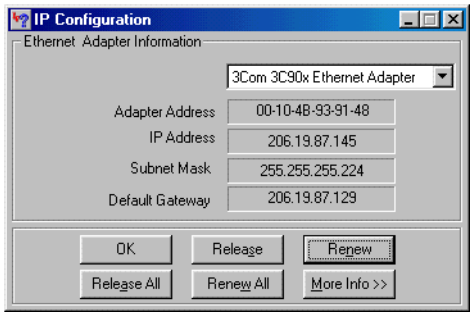
2 Select **Run**. The Run window is displayed.

3 Type **winipcfg.exe** and click **OK.** The IP Configuration window is displayed. The Ethernet Adapter Information field will vary depending on the system, as shown in the following examples:









The values for Adapter Address, IP Address, Subnet Mask, and Default Gateway on the PC will be different than in the image.

In Windows 98, if "Autoconfiguration" is displayed before the IP Address as in the following image, call your service provider.

4 Select the adapter name — the Ethernet card or USB device.

5 Click **Renew**.

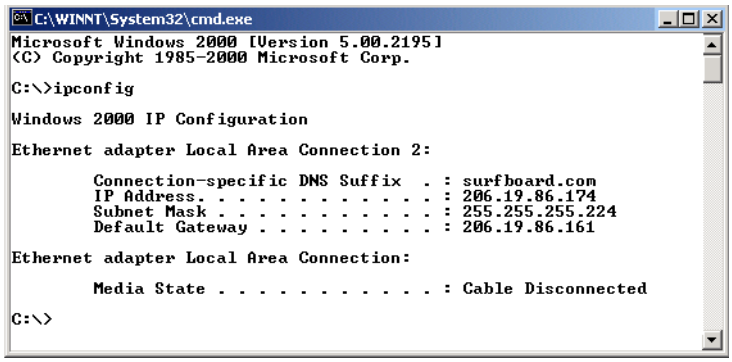
6 Click **OK** after the system displays an IP address.

If after performing this procedure the computer cannot access the Internet, call your cable service provider for help.

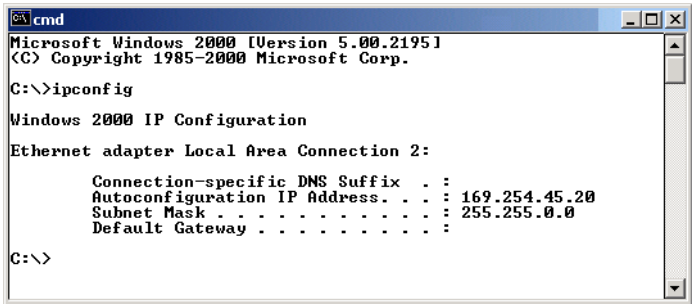
Verifying the IP Address in Windows 2000 or Windows XP

To check the IP address:

1. On the Windows Desktop, click **Start**.
2. Select **Run**. The Run window is displayed.
3. Type **cmd** and click **OK** to display a command prompt window.
4. Type **ipconfig** and press **ENTER** to display the IP configuration. A display similar to the following indicates a normal configuration:


C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . : surfboard.com
IP Address. . . . . : 206.19.86.174
Subnet Mask . . . . . : 255.255.255.224
Default Gateway . . . . . : 206.19.86.161
Ethernet adapter Local Area Connection:
Media State . . . . . : Cable Disconnected
C:\>

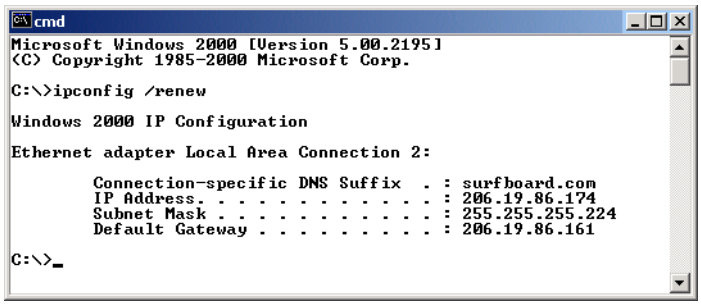
If an Autoconfiguration IP Address is displayed as in the following window, there is an incorrect connection between the PC and the SBG900 or there are cable network problems. Check the cable connections and determine if you can view cable-TV channels on your television:


cmd
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
Autoconfiguration IP Address. . . : 169.254.45.20
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
C:\>

After verifying the cable connections and proper cable-TV operation, renew the IP address.

To renew the IP address:

1 Type **ipconfig /renew** and press **ENTER**. If a valid IP address is displayed as shown, Internet access should be available.


cmd
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>ipconfig /renew
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . : surfboard.com
IP Address. . . . . : 206.19.86.174
Subnet Mask . . . . . : 255.255.255.224
Default Gateway . . . . . : 206.19.86.161
C:\>

2 Type **exit** and press **ENTER** to return to Windows.

If after performing this procedure the computer cannot access the Internet, call your cable service provider for help.

Setting Up the Wireless LAN

You can use the SBG900 as an access point for a wireless LAN without changing its default settings.

Caution!

The default SBG900 settings provide no wireless security. After your wireless LAN is operational, be sure to enable security as described in "Setting Up the Wireless LAN" in the SBG900 User Guide.

To enable security for your SBG900 wireless LAN, you can do the following on the SBG900:

To	Perform on the SBG900	Advantages	Disadvantages
Configure an Extended Service Set Identifier (ESSID) and enable closed network operation	Configuring the Wireless Network Name on the SBG900	Provides a unique name to distinguish from other nearby wireless LANs.	You must configure the ESSID on each client computer. Does not encrypt wireless data
Enable Wired Equivalent Privacy (WEP) encryption and configure a WEP key	Configuring WEP on the SBG900	Encrypts wireless data	You must configure the WEP key on each client computer.
Restrict access to computers with known MAC addresses	Configuring a MAC Access Control List on the SBG900	No configuration on client required No code that can be broken.	You must input each client MAC address on the SBG900 Does not encrypt wireless data

Connect at least one computer to the SBG900 Ethernet or USB port to use for performing configuration. Do not attempt to configure the SBG900 over a wireless connection.

You need to configure each wireless client station to access the SBG900 LAN as described in "Configuring the Wireless Clients".

Caution!

Never provide the ESSID or WEP key to anyone who is not authorized to use your wireless LAN.

For descriptions of all wireless configuration fields, see "Wireless Pages in the SBG900 Setup Program".

Another common-sense step to improve wireless security is to place wireless components away from windows. This decreases the signal strength outside the intended area.

Configuring the Wireless Network Name on the SBG900

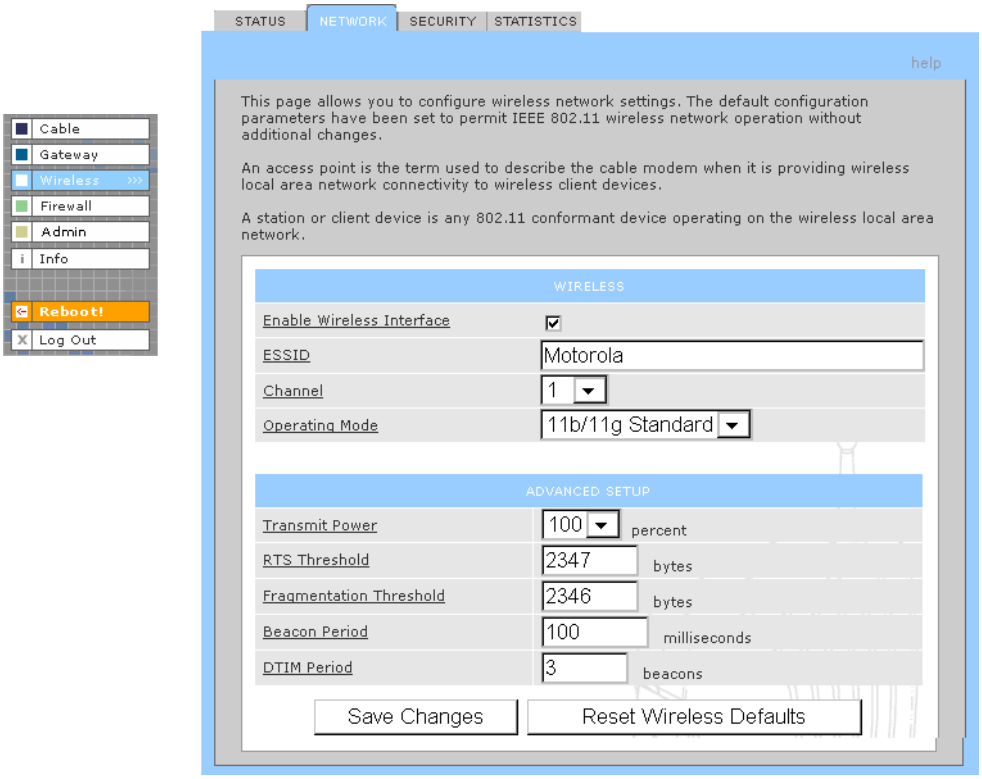
If you check Disable ESSID Broadcast on the SBG900 Wireless > SECURITY — advanced Page, you must configure the same network name (ESSID) on all wireless LAN clients (stations). Never provide the ESSID to anyone who is not authorized to use your wireless LAN.

To configure the ESSID:

1 Start the SBG900 Setup Program as described in "Starting the SBG900 Setup Program".

2 On the left frame, click **Wireless**.

3 Click the **NETWORK** tab to display:

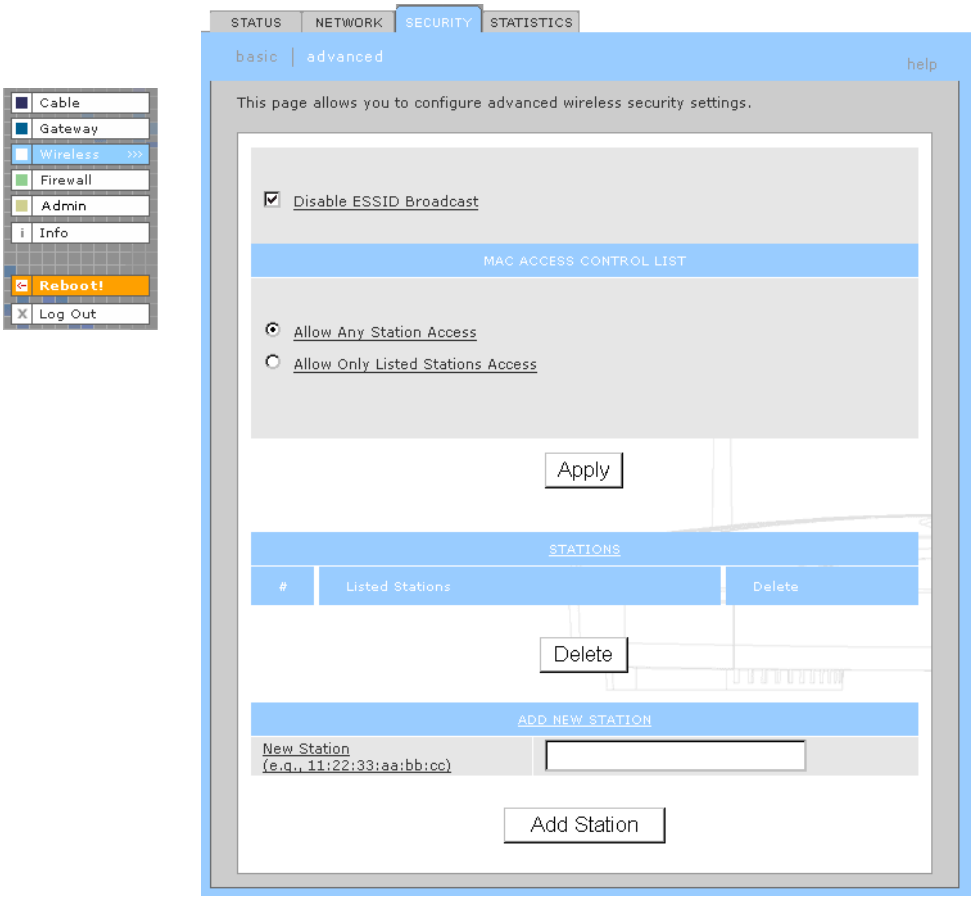


4 In the **ESSID** field, type a unique ***name***. It can be any alphanumeric, case-sensitive string up to 32 characters. The default is "Motorola." *Do not use the default ESSID.*

5 Click **Save Changes** to save your changes.

6 To restrict wireless LAN access to clients configured with the same Network Name (ESSID) as the SBG900, click the **SECURITY** tab.

7 Click **advanced** to display the Wireless > SECURITY — advanced Page*:*



8 Check **Disable ESSID Broadcast** to restrict wireless LAN access to clients configured with the same Network Name (ESSID) as the SBG900.

9 Click **Apply** to save your changes.

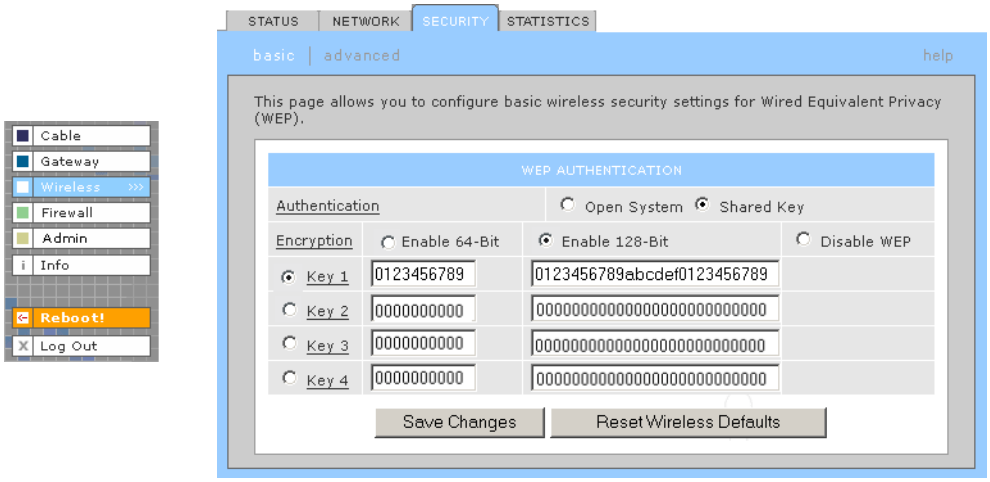
Configuring WEP on the SBG900

Caution!

> *The default settings provide no security for wireless data.* After the wireless LAN is operational, be sure to enable Shared Key Authentication and Wired Equivalent Privacy (WEP) encryption. You must configure the same WEP key on the SBG900 access point and all wireless clients (stations). *Never provide the WEP key to anyone who is not authorized to use the wireless LAN.*

To enable WEP and set the key on the SBG900:

1. On the SBG900 Setup Program left frame, click **Wireless**.
2. Click the **SECURITY** tab to display the Wireless > SECURITY — basic page:



3. Set the following:

Authentication — Sets whether shared key authentication is enabled to provide data privacy on the wireless LAN:

- Open System — Any wireless LAN client can transmit data to any other client without authentication. *Open authentication provides no security for transmitted data.* It is the default.
- Shared Key — All data transmitted over the wireless LAN is encrypted. The SBG900 authenticates and transfers data to and from all clients having shared key authentication enabled and an identical WEP key.

Encryption — Use a WEP key length that is compatible with your wireless client adapters. Choose *one* of:

- Enable 64-Bit — Use only if you have wireless clients that do not support 128-bit encryption
- Enable 128-Bit — The recommended setting for stronger encryption; supported by the Motorola PCC11b wireless card, USB11b wireless adapter, and most current wireless adapters
- Disable WEP — Recommended during network setup *only*

Key 1 to Key 4 — Sets the active WEP key. You can enter up to four 64-bit or 128-bit WEP *keys* containing the non-case-sensitive hexadecimal characters 0 to 9 and A to F. Only *one* key can be active:

- For 64-bit encryption, set the 10-character long key under Enable 64-Bit.
- For 128-bit encryption, set the 26-character long key under Enable 128-Bit.

For optimal security, we recommend changing the WEP keys frequently. Never provide the WEP key to anyone who is not authorized to use your wireless LAN.

4. If necessary, click **Reset Wireless Defaults** to reset the wireless defaults.
5. Click **Save Changes** to save your changes.

Configuring a MAC Access Control List on the SBG900

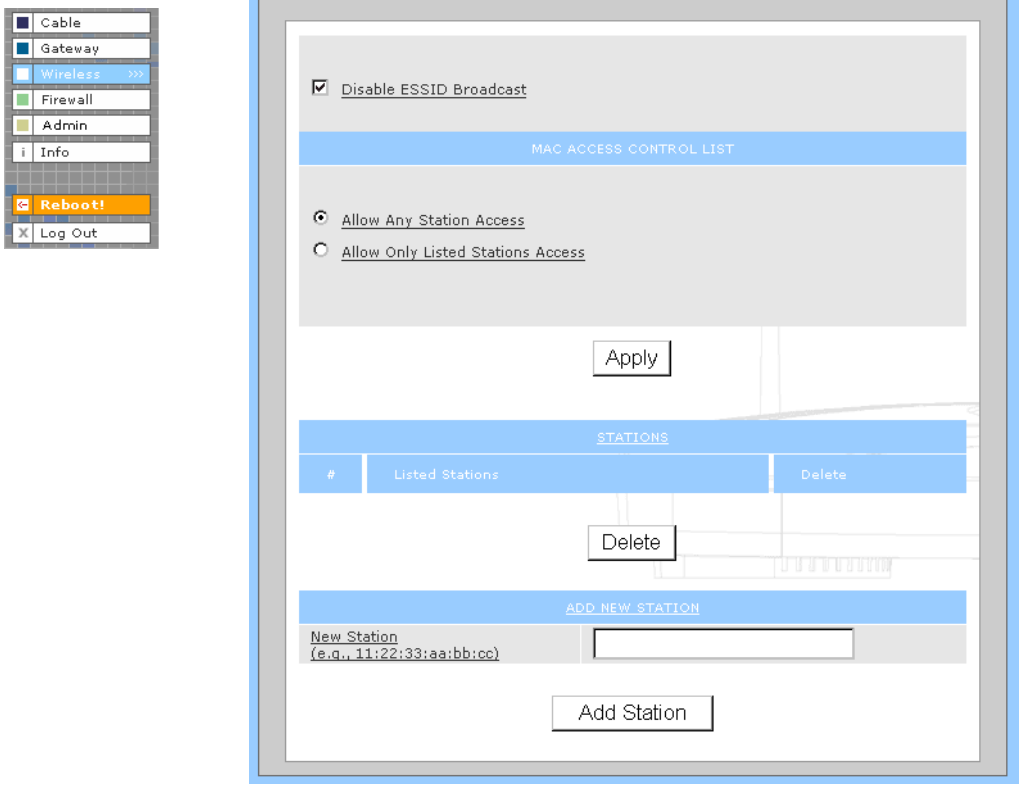
You can restrict wireless access to one to 32 wireless clients, based on the client MAC address.

To configure a MAC access control list:

1 On the SBG900 Setup Program left frame, click **Wireless**.

2 Click the **SECURITY** tab.

3 Click **advanced** to display the Wireless > SECURITY — advanced Page:



4 To restrict wireless access to systems in the MAC access control list, check **Allow Only Listed Stations Access** and click **Apply**.

5 To add a wireless client, type its MAC address in the format ***xx:xx:xx:xx:xx:xx*** in the **New Station** field and click **Add Station**.

You can add up to 32 wireless clients to the MAC access control list.

Configuring the Wireless Clients

For each wireless client computer (station), install the wireless adapter — such as a Motorola PCC11b wireless card or Motorola USB11b wireless adapter — following the instructions supplied with the adapter.

Configure the card or adapter to obtain an IP address automatically. The Motorola PCC11b wireless card and Motorola USB11b wireless adapter are supplied with a client configuration program called Wireless Client Manager, which is installed in the Windows Startup group.

If Wireless Client Manager is running, the icon is displayed on the Windows task bar. Double-click the icon to launch the utility.

After you correctly set the network name and WEP key on the client computer to match the SBG900, you should be able to use the computer to surf the Internet.

Configuring a Wireless Client with a Network Name (ESSID)

To distinguish it from other nearby wireless LANs, you can identify your wireless LAN with a unique network name (also known as a network identifier or ESSID). When prompted for the network identifier, network name, or ESSID, type the ***name*** set in the ESSID field on the Wireless > NETWORK Page in the SBG900 Setup Program. For more information, see "Configuring the Wireless Network Name on the SBG900".

After you specify the network name, many wireless cards or adapters automatically scan for an access point such as the SBG900 and the proper channel and data rate. If your card requires you to manually start scanning for an access point, do so following the instructions in the documentation supplied with the card.

Never provide the ESSID to anyone who is not authorized to use your wireless LAN.

Configuring a Wireless Client for WEP

If shared key Authentication is enabled and a WEP key is set on the SBG900 as described in "Configuring WEP on the SBG900", you must enter the same WEP key on the wireless client. The SBG900 cannot authenticate a client if:

- Shared key Authentication is enabled on the SBG900 but not on the client
- The client WEP key does not match the SBG900 WEP key

Caution!

If shared key authentication is not enabled and no WEP key is set, there is no encryption for wireless data. You must configure the same WEP key on the SBG900 and all wireless clients. *Never provide the WEP key to anyone who is not authorized to use your wireless LAN.*

Wireless Pages in the SBG900 Setup Program

Use the Wireless pages to control and monitor the wireless interface:

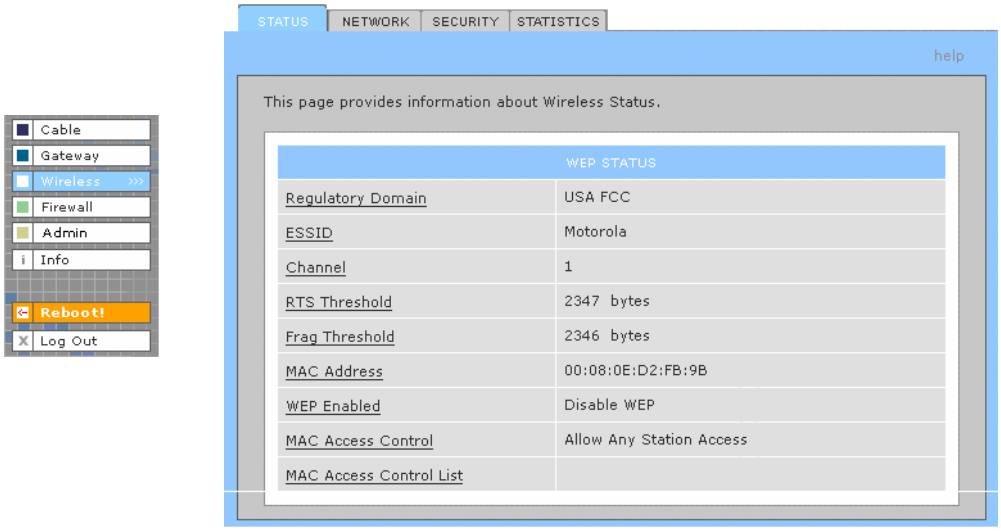
- Wireless > STATUS Page
- Wireless > NETWORK Page
- Wireless > SECURITY — basic Page
- Wireless > SECURITY — advanced Page
- Wireless > STATISTICS page

After you edit some fields and click Apply, you are warned that you must reboot for your change to take effect. Rebooting takes 10 to 15 seconds. After rebooting, you must log-in again.

Wireless > STATUS Page

You can use this display-only page to

- View the wireless interface status
- Help perform Troubleshooting for wireless network problems



Wireless > STATUS Page Fields

Regulatory Domain — Indicates the country the SBG900 is manufactured for. The list of channels depends on the country's standards for operation of wireless devices. Depending on the domain set at the factory, USA FCC, Europe, Spain, France, Japan, or some other country name is displayed.

ESSID — Displays the ESSID set on the Wireless > NETWORK Page. For more information, see "Configuring the Wireless Network Name on the SBG900". *Never provide the ESSID to anyone who is not authorized to use your wireless LAN.*

Channel — Displays the radio channel for the access point. If you encounter interference, you can set a different channel on the Wireless > NETWORK Page.

RTS Threshold — Displays the Request to Send Threshold set on the Wireless > NETWORK Page.

Frag Threshold — Displays the Fragmentation Threshold set on the Wireless > NETWORK Page.

MAC Address — Displays the SBG900 MAC address.

WEP Enabled — Displays the type of Wired Equivalent Privacy (WEP) that is enabled. For more information, see "Configuring WEP on the SBG900".

MAC Access Control — Displays the MAC Access Control setting set on the Wireless > SECURITY — advanced Page:

- Allow Listed — Only clients in the MAC access control list can access the wireless LAN.
- Allow Any Station Access — Any wireless client can access the wireless LAN.

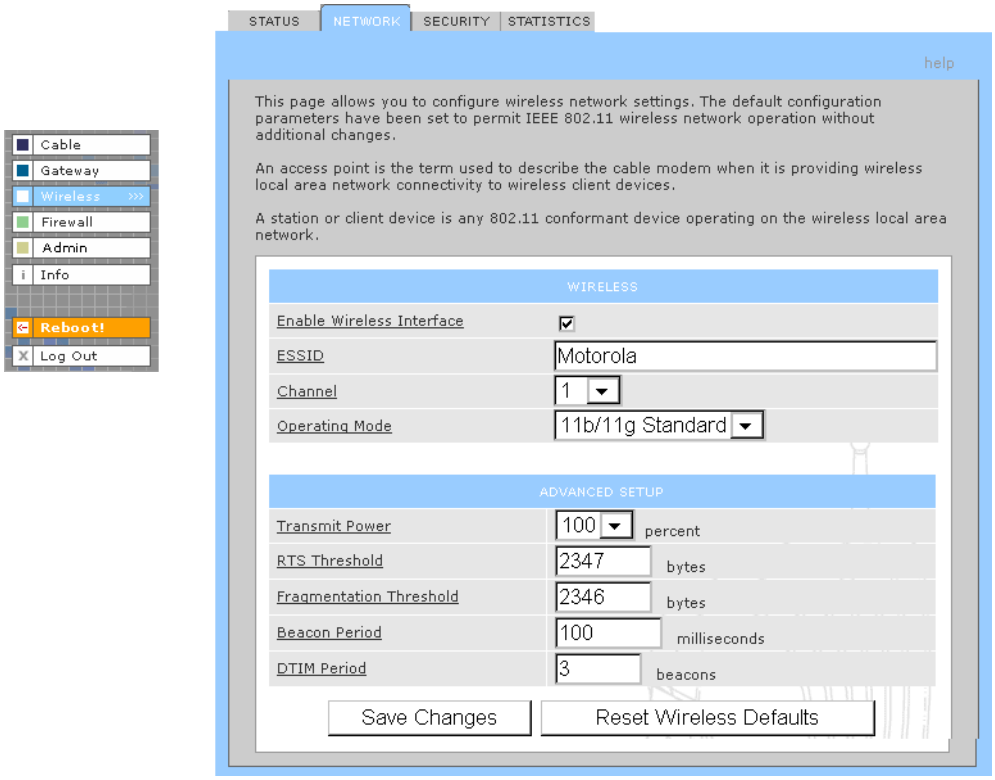
MAC Access Control List — Displays the MAC addresses of wireless clients having access. The list is set on the Wireless > SECURITY — advanced Page.

Wireless > NETWORK Page

Use this page for:

- Configuring the Wireless Network Name on the SBG900
- Configuring other wireless LAN settings

You can use the SBG900 to operate a wireless LAN without changing its default settings.



Wireless > NETWORK page fields

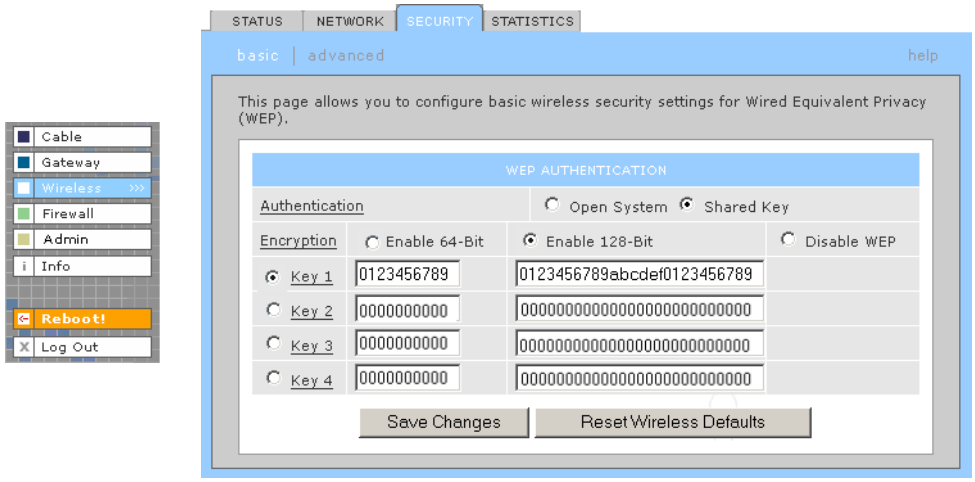
Field	Description
WIRELESS	
Enable Wireless Interface	Check this box to enable the wireless interface.
ESSID	Sets a unique network name for the SBG900 wireless LAN to distinguish between multiple wireless LANs in the vicinity. *If you check Disable ESSID Broadcast on the Wireless > SECURITY — advanced Page, all clients on the wireless LAN must have the same ESSID (network name) as the SBG900.* It can be any alphanumeric, case-sensitive string up to 32 characters. The default is "Motorola." *We strongly recommend not using the default. Never provide the ESSID to anyone who is not authorized to use your wireless LAN.*
Channel	Sets the wireless radio channel. You can change the channel if you encounter interference on the default channel. The default is 1 (one), except in countries where the first channel permitted for wireless operation is not one.

Wireless > NETWORK page fields (continued)

Field	Description
Operating Mode	Sets how the SBG900 communicates with wireless clients (stations): • 11b/11g Standard — Enables all IEEE 802.11b and IEEE 802.11g clients to work with the SBG900. *We recommend using this default setting in most cases because it is more flexible.* • 11g Enhanced — Choose this option only if all IEEE 802.11g clients on the network support the performance-enhancing features of the IEEE 11g Enhanced mode. It is not supported by all IEEE 802.11g stations.
ADVANCED SETUP	
Transmit Power	Sets the transmit power on the SBG900 wireless access point — 1, 2, 5, 10, 25, 50, or 100 mW. The default is 32 mW. Transmit power control is an optional IEEE 802.11b feature.
RTS Threshold	The Request To Send Threshold sets the packet size at which the access point issues an RTS before sending the packet. A low RTS can help when many clients are associated with the SBG900 or when the clients are far apart and can detect the SBG900 but not each other. It can be 0 to 2347 bytes. The default is 2347.
Fragmentation Threshold	Sets the size at which packets are fragmented (sent as several packets instead of as one packet). A low Fragmentation Threshold can help when communication is poor or when there is a significant interference. It can be 256 to 2346 bytes. The default is 2346.
Beacon Period	Sets the time between beacon frames sent by the SBG900 for wireless network synchronization. It can be from 1 to 999 ms. The default is 100 ms.
DTIM Period	The delivery traffic indication message (DTIM) period is the number of Beacon Periods that elapse before a wireless client operating in power save mode “listens” for buffered broadcast or multicast messages from the SBG900. It can be from 1 to 99999. The default is 3.

Wireless > SECURITY — basic Page

Use this page to configure basic Wired Equivalent Privacy (WEP) settings.



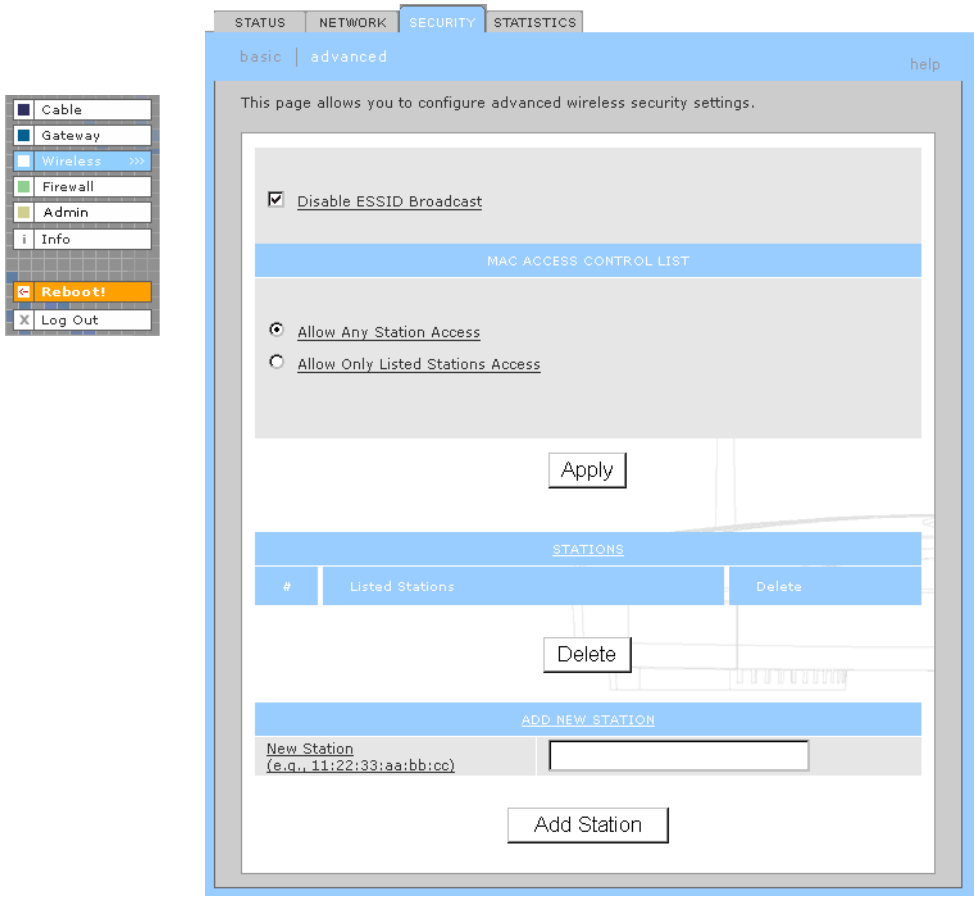
Caution!

The default Authentication setting Disable WEP provides no security for transmitted data.

For information about using this page, see "Configuring WEP on the SBG900".

Wireless > SECURITY — advanced Page

Use this page to configure advanced wireless security settings.



Wireless > Security — ADVANCED page fields

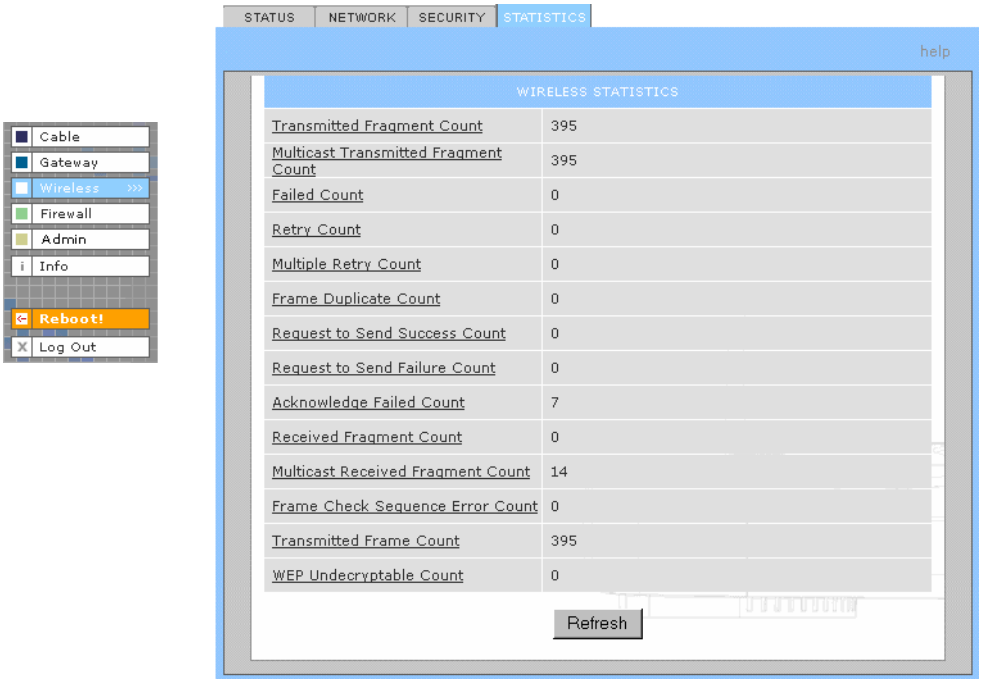
Field or Button	Description
Disable ESSID Broadcast	If checked, only wireless clients (stations) having the same Network Name (ESSID) as the SBG900 can communicate with the SBG900. Closed network operation is a SBG900 enhancement to IEEE 802.11b. The default is unchecked (off).
MAC ACCESS CONTROL LIST	You can restrict wireless access to one to 32 wireless clients, based on the client MAC address.
Allow Any Station Access	If checked, any wireless client can access the SBG900 wireless LAN.
Allow Only Listed Stations Access	If checked, only wireless clients in the MAC access control list can access the SBG900 wireless LAN.
Apply	Click to apply your change.
Listed Stations	Lists the wireless clients in the MAC access control list having access if Allow Only Listed Stations Access is checked.
Delete	To delete a wireless client from the MAC access control list, select its **Delete** check box and click the **Delete** button.

Wireless > Security — ADVANCED page fields (continued)

Field or Button	Description
ADD NEW STATION	
New Station	Type the MAC address of the wireless client to add to the MAC access control list. Use the format *xx:xx:xx:xx:xx:xx*. The MAC access control list can contain one to 32 clients.
Add Station	Click to add the New Station to the MAC access control list.

Wireless > STATISTICS page

Use this page to display wireless statistics.



Wireless > STATISTICS page fields

Field or Button	Description
Transmitted Fragment Count	The number of acknowledged MAC protocol data units (MPDUs) with an address in the address 1 field or an MPDU with a multicast address in the address 1 field of type data or management.
Multicast Transmitted Fragment Count	The number of transmitted fragments when the multicast bit is set in the destination MAC address of a successfully transmitted MAC service data unit (MSDU). When operating as a STA in an ESS, where these frames are directed to the AP, this implies having received an acknowledgment to all associated MPDUs.
Failed Count	The number of MSDUs not transmitted successfully because the number of transmit attempts exceeded the IEEE 802.11b short or long retry limit.
Retry Count	The number of successfully transmitted MSDUs after one or more retransmissions.

Wireless > STATISTICS page fields (continued)

Field or Button	Description
Multiple Retry Count	The number of successfully transmitted MSDUs after more than one retransmission.
Frame Duplicate Count	The number of frames received where the Sequence Control field indicated the frame was a duplicate.
Request To Send Success Count	The number of CTS messages received in response to RTS messages.
Request To Send Failure Count	The number of CTS messages not received in response to RTS messages.
Acknowledge Failed Count	The number of acknowledgment messages not received when expected from a data message transmission.
Received Fragment Count	The number of successfully received MPDUs of type Data or Management.
Multicast Received Fragment Count	The number of MSDUs received when the multicast bit was set in the destination MAC address.
Frame Check Sequence Error Count	The number of FCS errors detected in a received MPDU.
Transmitted Frame Count	The number of successfully transmitted MSDUs.
WEP Undecryptable Count	This number of frames received with the WEP subfield of the Frame Control field set to one and the WEP On key value mapped to the client MAC address. This indicates that the frame should not have been encrypted or was discarded due to the receiving client not having WEP enabled.
Refresh	Click to collect new data.

Setting Up a USB Driver

The following subsections describe setting up a USB driver if you connect a PC to the USB port on the SBG900. Perform one of the following procedures based on your Windows version:

- Setting Up a USB Driver in Windows 98
- Setting Up a USB Driver in Windows 2000
- Setting Up a USB Driver in Windows Me
- Setting Up a USB Driver in Windows XP

The SBG900 USB driver does not support Macintosh or UNIX computers. For those systems, you can connect through Ethernet *only*.

Caution!

Be sure the Motorola SURFboard Wireless Cable Modem Gateway CD-ROM is inserted in the CD-ROM drive before you plug in the USB cable.

If you have a problem setting up the USB driver, remove it by performing *one* of the following procedures:

- Removing the USB Driver from Windows 98 or Windows Me
- Removing the USB Driver from Windows 2000
- Removing the USB Driver from Windows XP

Setting Up a USB Driver in Windows 98

1 *Insert the Motorola SURFboard Wireless Cable Modem Gateway CD-ROM in the CD-ROM drive.* This CD contains the USB drivers and must be inserted and read by the PC before you connect the SBG900 to the PC.

2 Connect the USB cable as shown in USB Connection.

A few seconds after you complete the USB connection, the Add New Hardware Wizard window is displayed:

Add New Hardware Wizard
This wizard searches for new drivers for:
USB Composite Device
A device driver is a software program that makes a hardware device work.
< Back
Next >
Cancel

3 Click **Next**. The following window is displayed:

Add New Hardware Wizard
What do you want Windows to do?
Search for the best driver for your device. (Recommended).
Display a list of all the drivers in a specific location, so you can select the driver you want.
< Back
Next >
Cancel

4 Be sure “Search for the best driver for your device” is selected.

5 Click **Next**. The following window is displayed:

Add New Hardware Wizard
Windows will search for new drivers in its driver database on your hard drive, and in any of the following selected locations. Click Next to start the search.
Floppy disk drives
CD-ROM drive
Microsoft Windows Update
Specify a location:
D:\net3cusb.inf
Browse...
< Back
Next >
Cancel

Be sure “CD-ROM drive” is the only box checked.

6 Click **Next**. The message “Please wait while Windows searches for a new driver for this device” is displayed.

If the computer successfully locates the driver, you can skip to step 9.

If the computer does not locate the driver, the previous window is displayed again.

7 Select **Specify a location** and type the location of the CD-ROM drive:

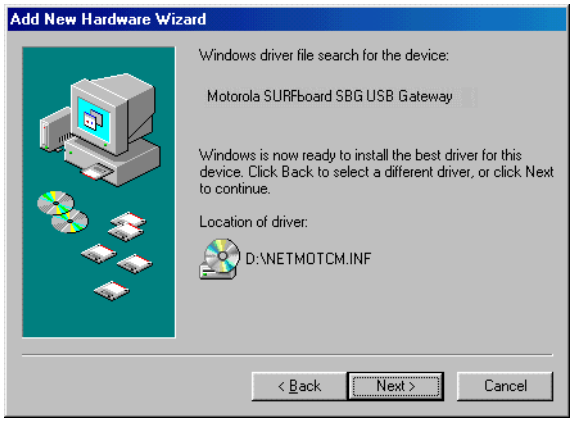
Add New Hardware Wizard
Windows will search for new drivers in its driver database on your hard drive, and in any of the following selected locations. Click Next to start the search.
Floppy disk drives
CD-ROM drive
Microsoft Windows Update
Specify a location:
D:\
Browse...
< Back
Next >
Cancel

To load the driver successfully, you may need to click **Browse** to manually select the NetMotCM.sys file on the CD-ROM.

8 Click **Next**. The following window is displayed:

Add New Hardware Wizard
Windows has found an updated driver for this device, and also some other drivers that should work with this device.
What do you want to install?
The updated driver (Recommended)
Motorola SURFboard SBG USB Gateway
One of the other drivers.
View List...
< Back
Next >
Cancel

9 Select **The updated driver...** and click **Next.** If the following window is not displayed, verify that the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM is properly inserted in the CD-ROM drive. If you still cannot find the correct driver file, click **Cancel** to cancel the installation and perform the procedure for "Removing the USB Driver from Windows 98 or Windows Me". Then repeat this procedure.

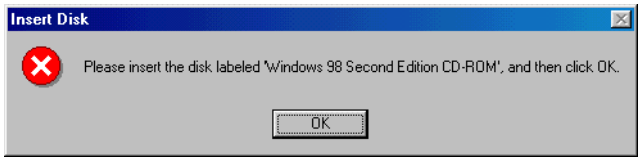

Add New Hardware Wizard
Windows driver file search for the device:
Motorola SURFboard SBG USB Gateway
Windows is now ready to install the best driver for this device. Click Back to select a different driver, or click Next to continue.
Location of driver:
D:\NETMOTCM.INF
< Back
Next >
Cancel

> Although your SBG model number may be different than in the images in this guide, the procedure is the same.

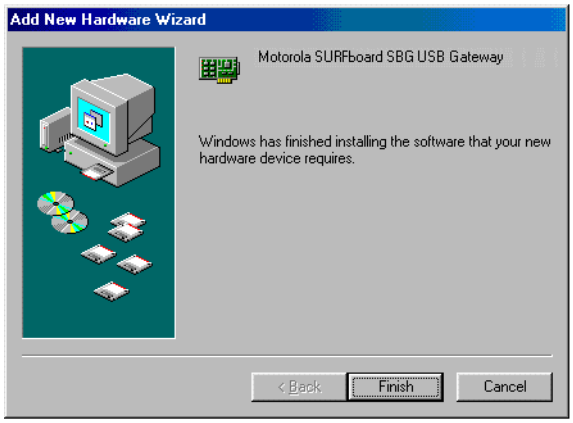
10 After the window shown under step 9 is displayed, click **Next**.

If a window with the message *Copying Files...* displays and asks for the CD-ROM drive, type the CD-ROM drive ***letter*** (for example, "D:") and click **OK**.

If an Insert Disk window similar to the one below is displayed, Windows 98 system files are needed to complete the installation. To install the files, insert your Windows 98 CD-ROM in the CD-ROM drive and click **OK**.



After all the necessary files are loaded, the following window is displayed to confirm a successful installation:


Add New Hardware Wizard
Motorola SURFboard SBG USB Gateway
Windows has finished installing the software that your new hardware device requires.
< Back
Finish
Cancel

11 Click **Finish.** The Systems Settings Change window is displayed:

System Settings Change
To finish setting up your new hardware, you must restart your computer.
Do you want to restart your computer now?
Yes
No

12 Click **Yes** to restart the computer.

When you finish setting up the USB driver, you can continue with "Configuring TCP/IP".

If you have difficulties setting up the USB driver, perform "Removing the USB Driver from Windows 98 or Windows Me" and repeat this procedure. If that does not correct the problem, see the *Regulatory, Safety, Software License, and Warranty Information* card provided with the SBG900 for information about obtaining warranty service.

Setting Up a USB Driver in Windows 2000

1 *Insert the Motorola SURFboard Wireless Cable Modem Gateway CD-ROM in the CD-ROM drive.* This CD contains the USB drivers and must be inserted and read by the PC before you connect the SBG900 to the PC.

2 Connect the USB cable as shown in USB Connection.

A few seconds after you complete the USB connection, the Found New Hardware window is displayed:

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install a device driver for a hardware device.
To continue, click Next.
< Back
Next >
Cancel

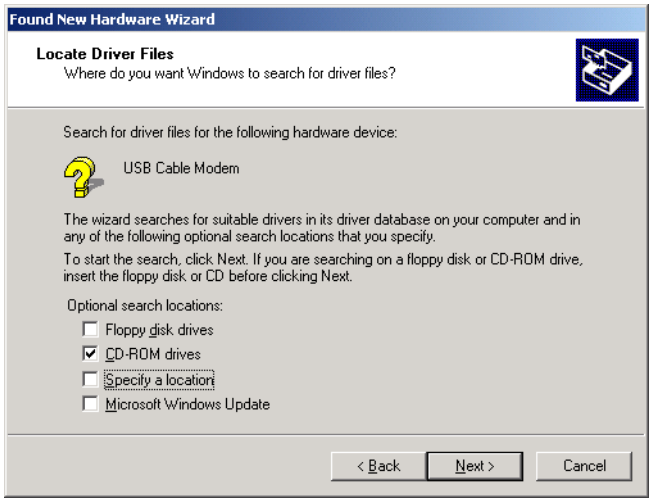
3 Click **Next**. The following window is displayed:

Found New Hardware Wizard
Install Hardware Device Drivers
A device driver is a software program that enables a hardware device to work with an operating system.
This wizard will complete the installation for this device:
USB Cable Modem
A device driver is a software program that makes a hardware device work. Windows needs driver files for your new device. To locate driver files and complete the installation click Next.
What do you want the wizard to do?
Search for a suitable driver for my device (recommended)
Display a list of the known drivers for this device so that I can choose a specific driver
< Back
Next >
Cancel

Although your SBG model number may be different than in the images in this guide, the procedure is the same.

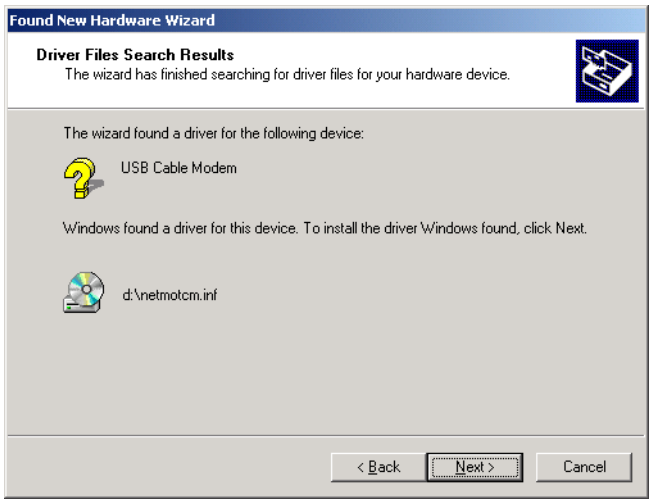
Be sure “Search for a suitable driver for my device” is selected.

4 Click **Next**. The following window is displayed:


Found New Hardware Wizard
Locate Driver Files
Where do you want Windows to search for driver files?
Search for driver files for the following hardware device:
USB Cable Modem
The wizard searches for suitable drivers in its driver database on your computer and in any of the following optional search locations that you specify.
To start the search, click Next. If you are searching on a floppy disk or CD-ROM drive, insert the floppy disk or CD before clicking Next.
Optional search locations:
Floppy disk drives
CD-ROM drives
Specify a location
Microsoft Windows Update
< Back
Next >
Cancel

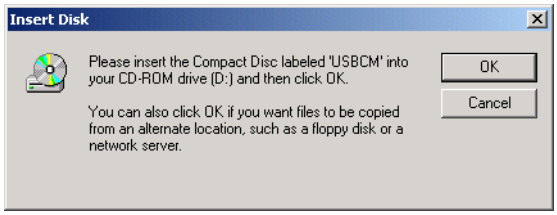
Be sure “CD-ROM drives” is the only box checked.

5 Click **Next**. The following window is displayed:

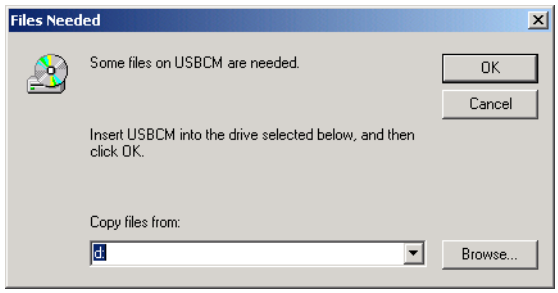

Found New Hardware Wizard
Driver Files Search Results
The wizard has finished searching for driver files for your hardware device.
The wizard found a driver for the following device:
USB Cable Modem
Windows found a driver for this device. To install the driver Windows found, click Next.
d:\netmotcm.inf
< Back
Next >
Cancel

6 Click **Next**.

If the Insert Disk window is displayed, be sure the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM is in the CD-ROM drive and follow steps 7 to 12. Otherwise, you can skip to step 13.


Insert Disk
Please insert the Compact Disc labeled 'USBCM' into your CD-ROM drive (D:) and then click OK.
You can also click OK if you want files to be copied from an alternate location, such as a floppy disk or a network server.
OK
Cancel

7 On the Insert Disk window, click **OK**. The Files Needed window is displayed:



8 If necessary, select the CD-ROM drive in the Copy files from list.

9 Click **Browse**.

10 Locate the NetMotCM.sys file in the CD-ROM root directory.

11 Double-click the **NetMotCM.sys** file. The Files Needed window is displayed.

12 Click **OK**. The Found New Hardware Wizard window is displayed:

Found New Hardware Wizard
Completing the Found New Hardware Wizard
Motorola SURFboard SBG USB Gateway
Windows has finished installing the software for this device.
To close this wizard, click Finish.
< Back
Finish
Cancel

13 Click **Finish** to complete the installation.

When you finish setting up the USB driver, you can continue with "Configuring TCP/IP".

If you have any difficulties setting up the USB driver, perform "Removing the USB Driver from Windows 2000" and repeat this procedure.

Setting Up a USB Driver in Windows Me

1 *Insert the Motorola SURFboard Wireless Cable Modem Gateway CD-ROM in the CD-ROM drive.* This CD contains the USB drivers and must be inserted and read by the PC before you connect the SBG900 to the PC.

2 Connect the USB cable as shown in USB Connection.

A few seconds after you complete the USB connection, the Add New Hardware Wizard window is displayed:

Add New Hardware Wizard
Windows has found the following new hardware:
USB Cable Modem
Windows can automatically search for and install software that supports your hardware. If your hardware came with installation media, insert it now and click Next.
What would you like to do?
Automatic search for a better driver (Recommended)
Specify the location of the driver (Advanced)
< Back
Next >
Cancel

3 Click **Next**. Windows automatically searches for the correct USB drivers and installs them. If the installation is successful, the following window is displayed:

> Although your SBG model number may be different than in the images in this guide, the procedure is the same.

4 If the window above is displayed, click **Finish**. Otherwise, be sure the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM is correctly inserted in the CD-ROM drive.

When you finish setting up the USB driver, you can continue with "Configuring TCP/IP".

Setting Up a USB Driver in Windows XP

1 *Insert the Motorola SURFboard Wireless Cable Modem Gateway CD-ROM in the CD-ROM drive.* This CD contains the USB drivers and must be inserted and read by the PC before you connect the SBG900 to the PC.

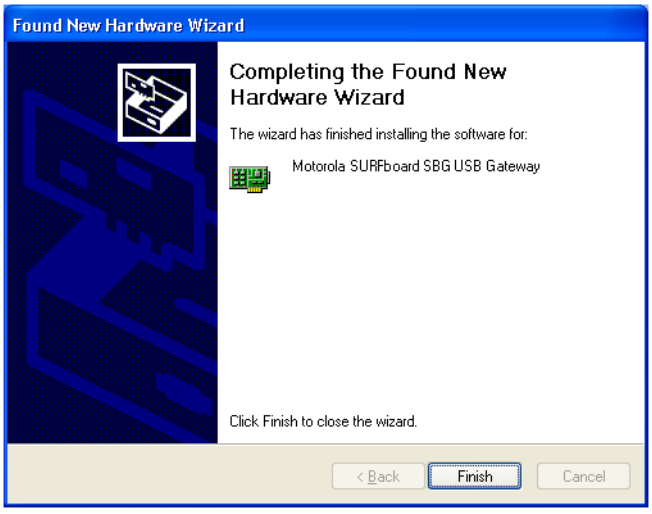
2 Connect the USB cable as shown in USB Connection.

A few seconds after you complete the USB connection, the Found New Hardware Wizard window is displayed:

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install software for:
USB Cable Modem
If your hardware came with an installation CD or floppy disk, insert it now.
What do you want the wizard to do?
Install the software automatically (Recommended)
Install from a list or specific location (Advanced)
Click Next to continue.
< Back
Next >
Cancel

3 Be sure “Install the software automatically” is selected.

4 Click **Next**. Windows automatically searches for the correct USB drivers and installs them. If the installation is successful, the following window is displayed:


Found New Hardware Wizard
Completing the Found New Hardware Wizard
The wizard has finished installing the software for:
Motorola SURFboard SBG USB Gateway
Click Finish to close the wizard.
< Back
Finish
Cancel

Although your SBG model number may be different than in the images in this guide, the procedure is the same.

5 Click **Finish** to complete the installation. Otherwise, be sure the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM is correctly inserted in the CD-ROM drive.

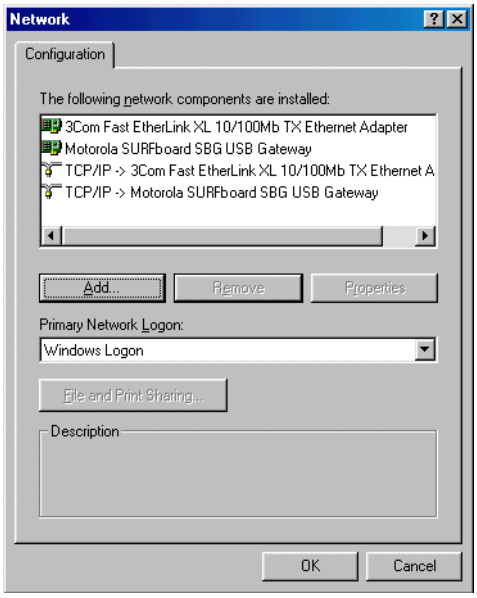
When you finish setting up the USB driver, you can continue with "Configuring TCP/IP".

Removing the USB Driver from Windows 98 or Windows Me

1 On the Windows Desktop, right-click *one* of:

- In Windows 98, the **Network Neighborhood** icon
- In Windows ME, the **My Network Places** icon

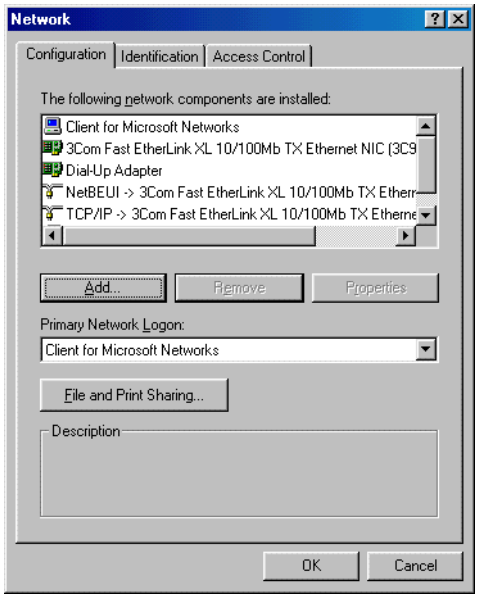
The Network window is displayed:



Although your SBG model number may be different than in the images in this guide, the procedure is the same.

2 Click the **Motorola SURFboard SBG900 USB Gateway**.

3 Click **Remove.** The Network window no longer displays Motorola SURFboard SBG900 USB Gateway in the list:



4 Click **OK**. The System Settings Change window is displayed:

System Settings Change
To finish setting up your new hardware, you must restart your computer.
Do you want to restart your computer now?
Yes
No

5 *Disconnect the USB cable from the PC or SBG900.*

6 Click **Yes** to restart the computer.

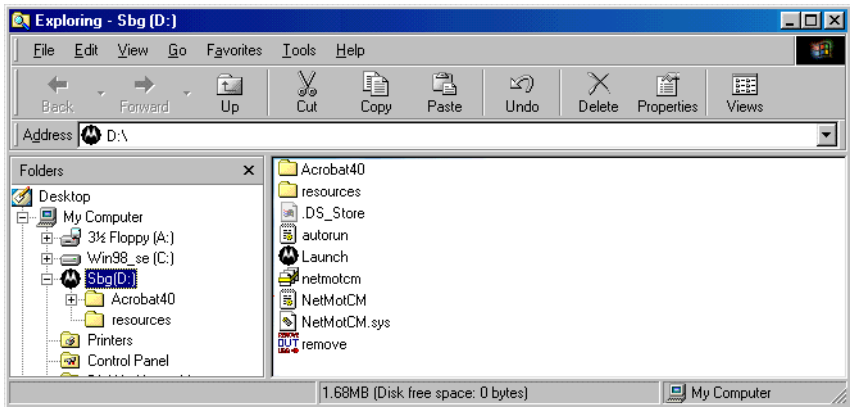
7 Insert the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM in the CD-ROM drive. After a short time, a window with language choices is displayed.

8 Press the **Esc** key on the keyboard to exit the start-up screens.

9 To start Windows Explorer, click **Start** and select **Run** to display the Run window.

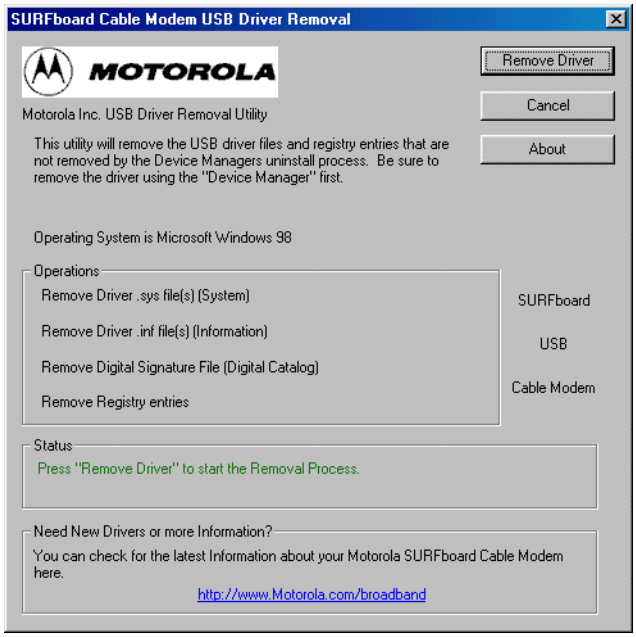
10 Type **explorer** and click **OK.**

The Exploring window is displayed. *Windows Explorer may appear different than in the image. There are variations between Windows versions and you can configure Windows Explorer as you like.*



11 Double-click the **Motorola SBG900** CD-ROM drive (D: in the image above).

12 Double-click **remove** or **remove.exe** to run the Remove utility from the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM. The SURFboard Cable Modem USB Driver Removal window is displayed:


SURFboard Cable Modem USB Driver Removal
MOTOROLA
Motorola Inc. USB Driver Removal Utility
This utility will remove the USB driver files and registry entries that are not removed by the Device Managers uninstall process. Be sure to remove the driver using the "Device Manager" first.
Remove Driver
Cancel
About
Operating System is Microsoft Windows 98
Operations
Remove Driver .sys file(s) (System)
Remove Driver .inf file(s) (Information)
Remove Digital Signature File (Digital Catalog)
Remove Registry entries
SURFboard
USB
Cable Modem
Status
Press "Remove Driver" to start the Removal Process.
Need New Drivers or more Information?
You can check for the latest Information about your Motorola SURFboard Cable Modem here.
http://www.Motorola.com/broadband

13 Click **Remove Driver**.

After you remove the USB driver, re-install it on the computer. Perform *one* of:

- Setting Up a USB Driver in Windows 98
- Setting Up a USB Driver in Windows Me

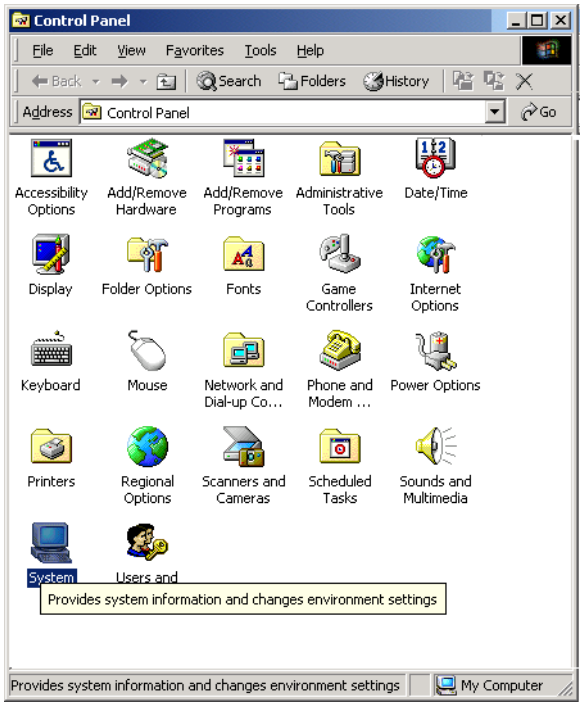
If you continue to have problems, contact your cable service provider.

Removing the USB Driver from Windows 2000

1 On the Windows desktop, click **Start**.

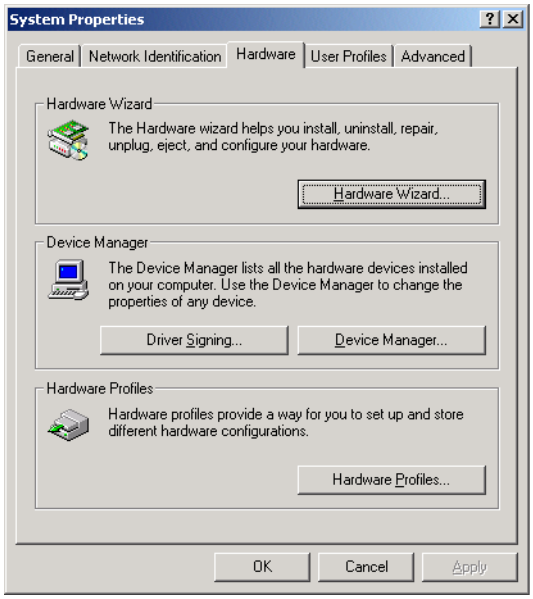
2 Click **Settings**.

3 Click **Control Panel** to display the Control Panel window:

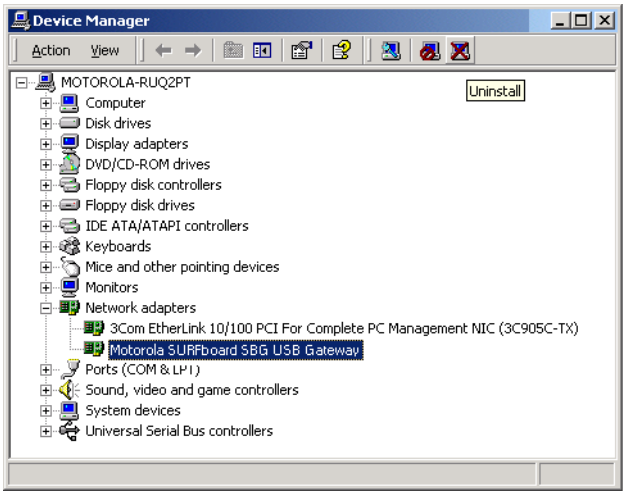


4 Double-click **System** to display the System Properties window.

5 Click the **Hardware** tab:


System Properties
General Network Identification Hardware User Profiles Advanced
Hardware Wizard
The Hardware wizard helps you install, uninstall, repair, unplug, eject, and configure your hardware.
Hardware Wizard...
Device Manager
The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.
Driver Signing...
Device Manager...
Hardware Profiles
Hardware profiles provide a way for you to set up and store different hardware configurations.
Hardware Profiles...
OK
Cancel
Apply

6 Click **Device Manager** to display the Device Manager window:



Although your SBG model number may be different than in the images in this guide, the procedure is the same.

7 Double-click **Network Adapters**.

8 Click the **Motorola SURFboard SBG900 USB Gateway**. The Uninstall icon displays on the window near the top.

9 Click the **Uninstall** icon. The following window is displayed:

Confirm Device Removal
Motorola SURFboard SBG USB Gateway
Warning: You are about to uninstall this device from your system.
OK
Cancel

10 Click **OK**.

11 Close the Device Manager window.

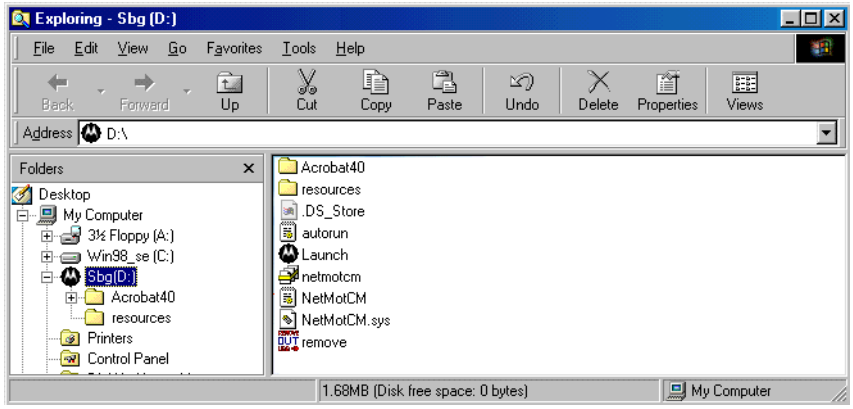
12 Close the Control Panel window.

13 Insert the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM in the CD-ROM drive.

14 Press the **Esc** key on the keyboard to exit the start-up screens.

15 To start Windows Explorer, click **Start** and select **Run** to display the Run window.

16 On the Run window, type **explorer** and click **OK** to display Windows Explorer:

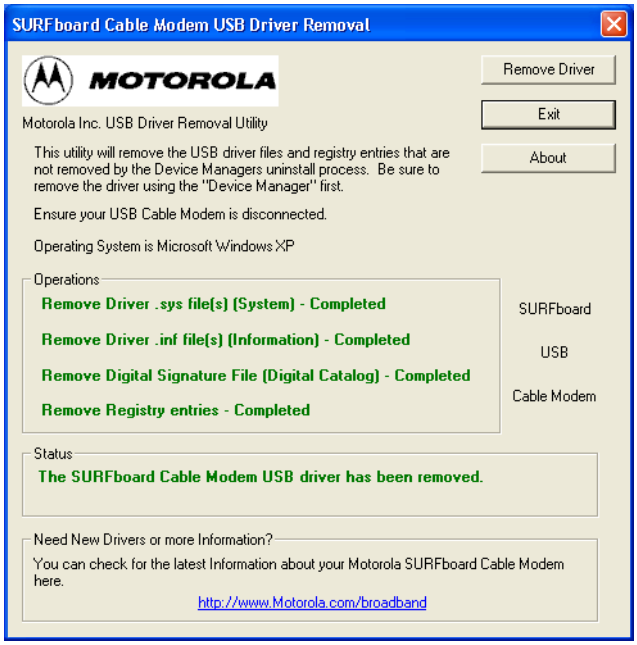


Windows Explorer may appear different than in the image. There are variations between Windows versions and you can configure Windows Explorer as you like.

17 Double-click **My Computer**.

18 Double-click the **Motorola SBG900** CD icon (D: in the image).

19 Double-click **remove** or **remove.exe** to run the Remove utility from the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM. The SURFboard Cable Modem USB Driver Removal window is displayed:


SURFboard Cable Modem USB Driver Removal
MOTOROLA
Motorola Inc. USB Driver Removal Utility
Remove Driver
Exit
About
This utility will remove the USB driver files and registry entries that are not removed by the Device Managers uninstall process. Be sure to remove the driver using the "Device Manager" first.
Ensure your USB Cable Modem is disconnected.
Operating System is Microsoft Windows XP
Operations
Remove Driver .sys file(s) (System) - Completed
Remove Driver .inf file(s) (Information) - Completed
Remove Digital Signature File (Digital Catalog) - Completed
Remove Registry entries - Completed
SURFboard
USB
Cable Modem
Status
The SURFboard Cable Modem USB driver has been removed.
Need New Drivers or more Information?
You can check for the latest Information about your Motorola SURFboard Cable Modem here.
http://www.Motorola.com/broadband

20 *Be sure the USB cable is disconnected.*

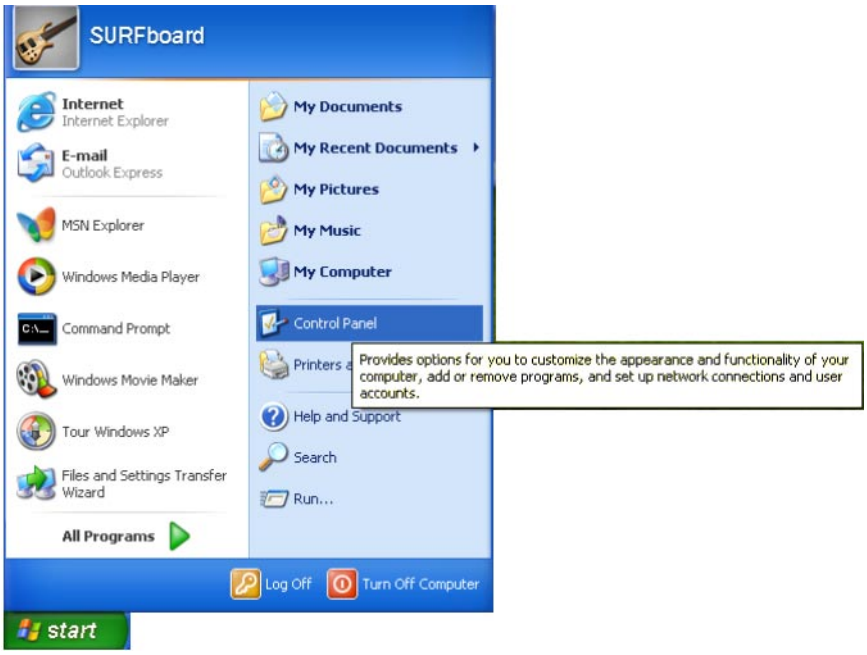
21 Click **Remove Driver.**

Informational messages similar to the ones shown are displayed on the SURFboard Cable Modem USB Driver Removal window.

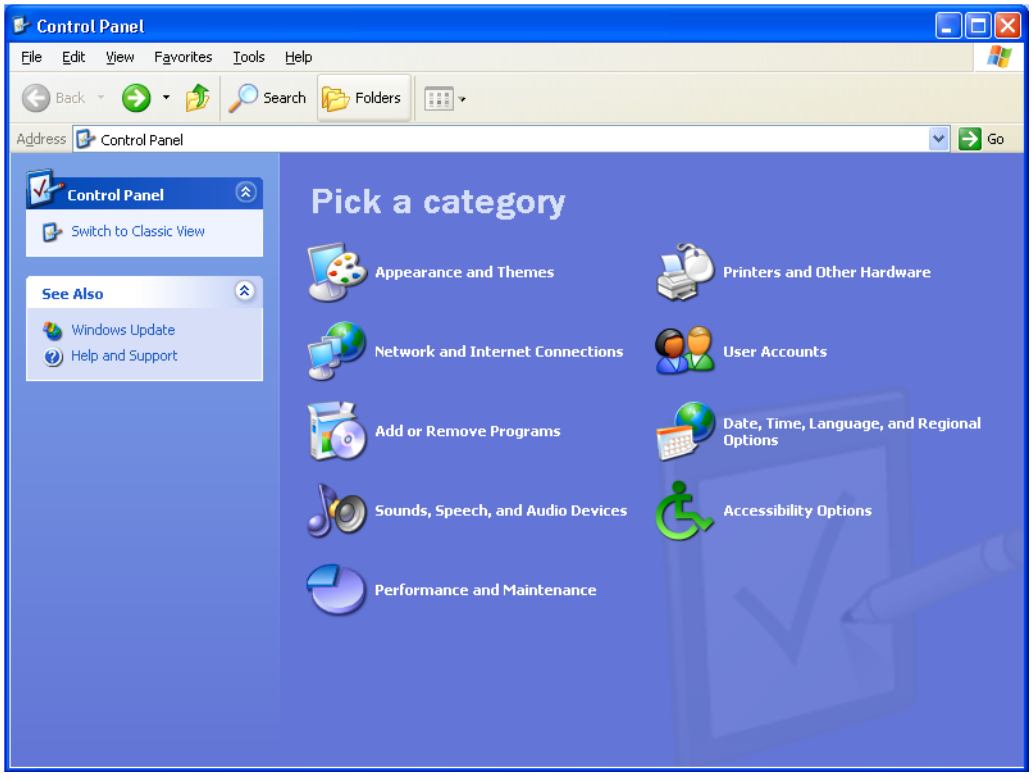
After you remove the USB driver, re-install it following "Setting Up a USB Driver in Windows 2000". If you continue to have problems, contact your cable service provider.

Removing the USB Driver from Windows XP

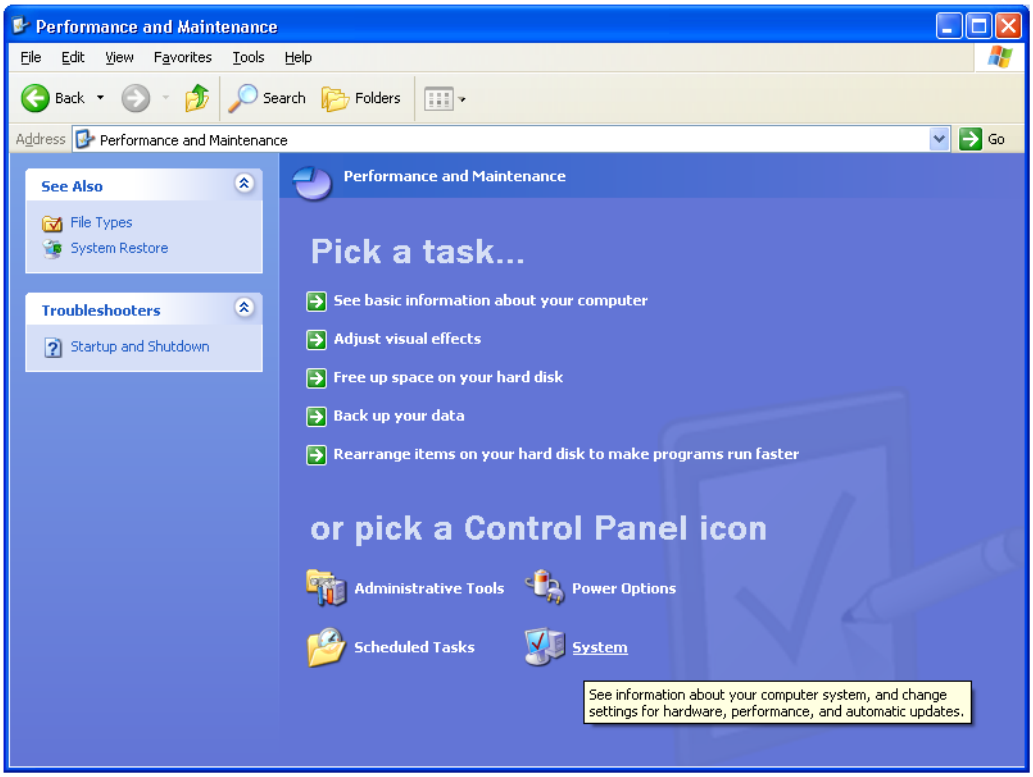
1 On the Windows desktop, click **Start** to display the Start window:



2 Click **Control Panel** to display the Control Panel window. The display varies, depending on the Windows XP view options:

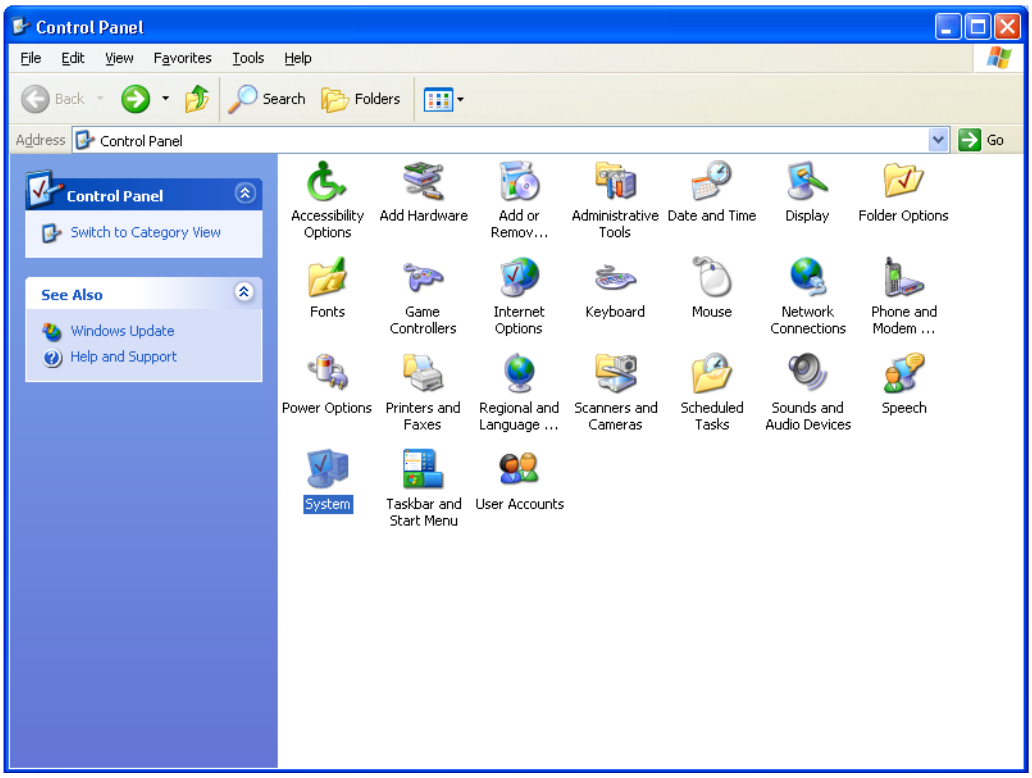


3 If a Category view similar to the image under step 2 is displayed, click **Performance and Maintenance** to display the Performance and Maintenance window. Otherwise, skip to step 5.

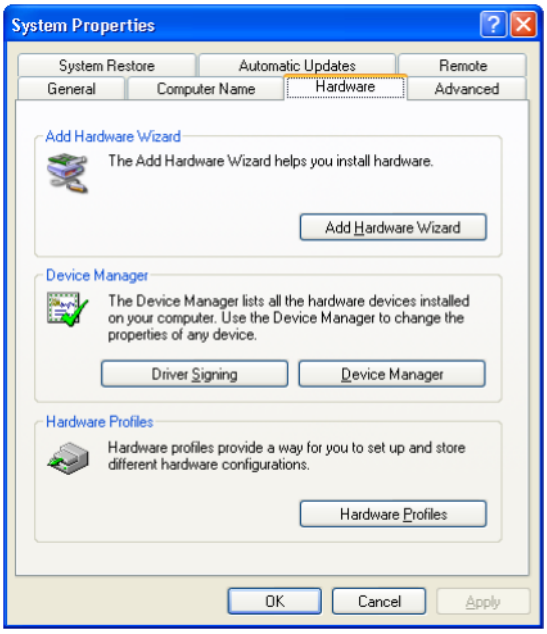

Performance and Maintenance
File Edit View Favorites Tools Help
Back Search Folders
Address Performance and Maintenance
Go
See Also
File Types
System Restore
Troubleshooters
Startup and Shutdown
Performance and Maintenance
Pick a task...
See basic information about your computer
Adjust visual effects
Free up space on your hard disk
Back up your data
Rearrange items on your hard disk to make programs run faster
or pick a Control Panel icon
Administrative Tools
Power Options
Scheduled Tasks
System
See information about your computer system, and change settings for hardware, performance, and automatic updates.

4 Click **System** to display the System Properties window. Skip to step 6.

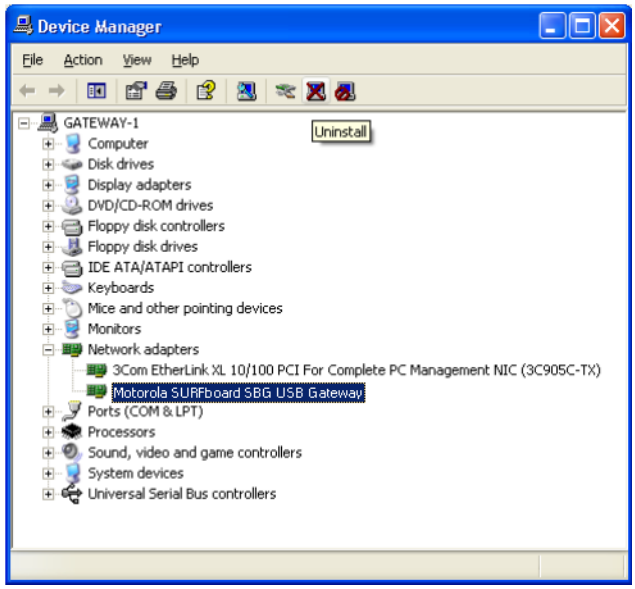
5 If a classic view similar to the following is displayed, click System to display the System Properties window:



6 Click the **Hardware** tab to display the Hardware page:



7 Double-click the **Device Manager** button to display the Device Manager window:



Although your SBG model number may be different than in the images in this guide, the procedure is the same.

8 Double-click **Network adapters**.

9 Click the **Motorola SURFboard SBG900 USB Gateway**. The Uninstall icon displays on the window near the top.

10 Click the **Uninstall** icon.

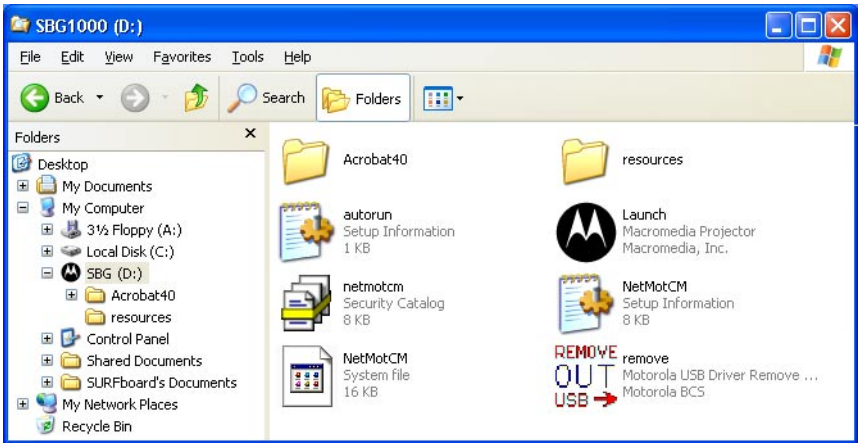
11 Close the Device Manager and Control Panel windows.

12 Insert the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM in the CD-ROM drive. After a short time, a window with language choices is displayed.

13 Press the **Esc** key on the keyboard to exit the start-up screens.

14 To start Windows Explorer, click **Start** and select **Run** to display the Run window.

15 Type **explorer** and click **OK** to display Windows Explorer.

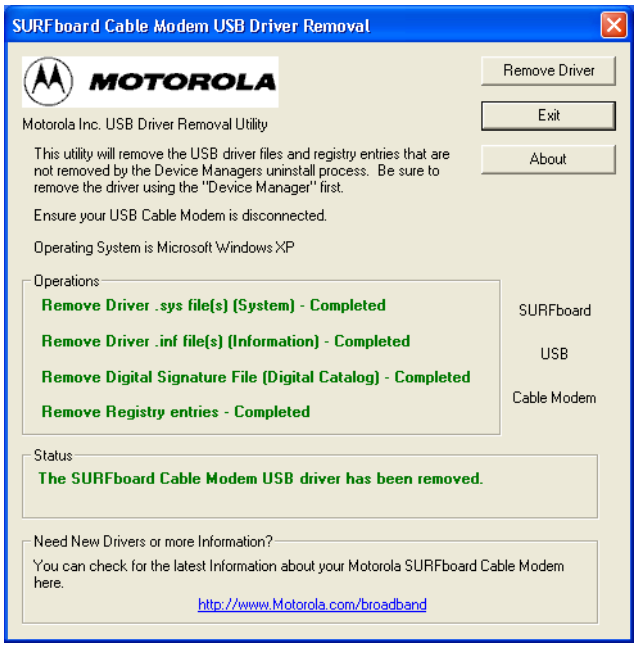


Windows Explorer may appear slightly different than in the image. There are variations between Windows versions and you can configure Windows Explorer as you like.

16 Double-click **My Computer**.

17 Double-click the **Motorola** CD icon (D: in the image).

18 Double-click **remove** or **remove.exe** to run the Remove utility from the *Motorola SURFboard Wireless Cable Modem Gateway* CD-ROM. The SURFboard Cable Modem USB Driver Removal window is displayed:


SURFboard Cable Modem USB Driver Removal
MOTOROLA
Motorola Inc. USB Driver Removal Utility
Remove Driver
Exit
About
This utility will remove the USB driver files and registry entries that are not removed by the Device Managers uninstall process. Be sure to remove the driver using the "Device Manager" first.
Ensure your USB Cable Modem is disconnected.
Operating System is Microsoft Windows XP
Operations
Remove Driver .sys file(s) (System) - Completed
Remove Driver .inf file(s) (Information) - Completed
Remove Digital Signature File (Digital Catalog) - Completed
Remove Registry entries - Completed
SURFboard
USB
Cable Modem
Status
The SURFboard Cable Modem USB driver has been removed.
Need New Drivers or more Information?
You can check for the latest Information about your Motorola SURFboard Cable Modem here.
http://www.Motorola.com/broadband

19 Be sure the USB cable is disconnected.

20 Click **Remove Driver.** Informational messages are displayed on the SURFboard Cable Modem USB Driver Removal window.

After you remove the USB driver, re-install it following "Setting Up a USB Driver in Windows XP". If you continue to have problems, contact your cable service provider.

Troubleshooting

If the solutions listed here do not solve your problem, contact your cable service provider. Before calling your cable service provider, try pressing the reset button on the rear panel. Resetting the SBG900 may take 5 to 30 minutes. Your service provider may ask for the status of the front-panel lights as described in Front-Panel Lights and Error Conditions.

Problem	Possible Solutions
POWER light is off	Check that the SBG900 is properly plugged into the electrical outlet. Check that the electrical outlet is working. Press the Reset button.
Cannot send or receive data	On the top front panel, note which is the first light (starting from the left) that is off. This light indicates where the error occurred as described in the "Front-Panel Lights and Error Conditions" table. If you have cable TV, check that the TV is working and the picture is clear. If you cannot receive regular TV channels, the data service will not function. Check the coaxial cable at the SBG900 and wall outlet. Hand-tighten if necessary. Check the IP address. Follow the steps for verifying the IP address for your system. See Configuring TCP/IP. Call your cable service provider if you need an IP address. Check that the Ethernet cable is properly connected to the SBG900 and the computer.
Problems related to unsuccessful USB driver installation	Remove the USB driver. Follow the appropriate procedure for your system in "Setting Up a USB Driver".
The SBG900 Setup Program will not start	The web cache is full or close to full. In Internet Explorer, choose **Internet Options** from the **Tools** menu, and click the **General** tab. Click **Delete Files** and **Clear History**. Then try Starting the SBG900 Setup Program again.
A wireless client(s) cannot send or receive data	Perform the first four checks in "Cannot send or receive data." Check whether the wireless interface is enabled. Check whether you configured the ESSID and disabled ESSID broadcasting on the SBG900. Then be sure the network name (ESSID) on each affected wireless client is identical to the ESSID on the SBG900. Check whether you configured a WEP key on the SBG900. If you configured a WEP key on the SBG900, be sure each affected wireless client has the identical WEP key. If this does not solve the problem, check whether the client wireless adapter supports the type of WEP key configured on the SBG900. Check whether you enabled Allow Only Listed Stations Access. If you did, be sure the MAC address for each affected wireless client is correctly listed. For detailed information, see "Setting Up the Wireless LAN".

Front-Panel Lights and Error Conditions

Light	Turns Off During Startup If	Turns Off During Normal Operation If
RECEIVE	The receive channel cannot be acquired	The receive channel is lost
SEND	The send channel cannot be acquired	The send channel is lost
ONLINE	IP registration is unsuccessful	The IP registration is lost
POWER	The SBG900 is not properly plugged into the power outlet	The SBG900 is unplugged

Contact Us

In the United States and Canada, if you need assistance while working with the SBG900 and related equipment supplied by Motorola:

If you rent or lease your SBG900	Contact your cable service provider.
If you own your SBG900	Call **1-877-466-8646** for technical and warranty support. Support is available 24 hours a day, seven days a week.

For information about customer service, technical support, or warranty claims, see the *Regulatory, Safety, Software License, and Warranty Information* card provided with the SURFboard SBG900.

For answers to typical questions, see “Frequently-Asked Questions”.

For more information about Motorola consumer cable products, education, and support, visit http://broadband.motorola.com.

Frequently-Asked Questions

Here are answers to questions our customers frequently ask:

Q What is high-speed cable Internet access?

A Cable Internet access uses cable television wires instead of telephone lines to connect to the Internet. It is extremely fast and does not tie up telephone lines for incoming or outgoing calls and faxes.

Q How fast is the Motorola SURFboard Cable Modem Gateway?

A Cable modems offer Internet access at speeds up to 100 times faster than a traditional phone modem. You can experience speeds of over 1,000 Kbps. Due to network condition such as traffic volume and the speed of the sites you visit, actual speed may vary. Many network and other factors can affect download speeds.

Q How many users can one SBG900 support?

A A single SBG900 can support up to 253 users, each assigned a unique IP address, on a Class C network.

Q What is Network Address Translation?

A NAT is a technique to translate private IP addresses on your LAN to a single IP address assigned by your cable service provider that is that is visible to outside users on the Internet.

Q What are IEEE 802.11g and IEEE 802.11b?

A They are IEEE wireless network standards.

Q What type of firewall is provided on the SBG900?

A The SBG900 provides a stateful-inspection firewall.

Q What wireless security measures are provided on the SBG900?

A To protect data transmitted over wireless connections, the SBG900 supports WEP encryption and MAC access control lists. For information, see "Setting Up the Wireless LAN".

Q Why is there no Standby button?

A As a security measure, current Motorola SURFboard cable modems provide a Standby button to temporarily suspend the Internet connection. Because the SBG900 firewall provides high security levels while connected, the Standby button is not required.

Q Can I still watch cable TV while using my Motorola SURFboard Cable Modem Gateway?

A Yes, your cable TV line can carry the TV signal while you send and receive information on the Internet.

Q What are CableLabs Certified, DOCSIS, and Euro-DOCSIS?

A CableLabs Certified, DOCSIS, and Euro-DOCSIS are the industry standards for high-speed data distribution over cable television system networks. They are intended to ensure that all compliant cable modems interface with all compliant cable systems. Your SBG900 is DOCSIS or Euro-DOCSIS certified.

Q If I have an SBG900, can I still use my old 28.8 Kbps or 56 Kbps modem?

A Yes you can. However, once you've experienced the speed of cable Internet access, you'll never again want to wait for traditional dial-up services.

Q **Do I need to change my Internet service provider (ISP)?**

A Currently, most Internet service providers do not provide cable Internet access. Contact your cable company for your specific information.

Q **Do I need to subscribe to cable TV to get cable Internet access?**

A No, but you will need to subscribe to cable Internet service. Some systems require that you subscribe to basic service before you can get Internet access and/or offer a discount when you use your own SBG900. Check with your local cable company for specific information.

Q **What type of technical support is available?**

A For questions about your Internet service, connection, or SBG900, call your cable service provider.

Q **What do I do if my SBG900 stops working?**

A "Troubleshooting" provides tips to diagnose problems and simple solutions. If you continue to have problems, call your cable service provider.

Q **Can multiple game players on the SBG900 LAN log onto the same game server and play simultaneously with just one public IP address?**

A It depends on the game server.

Specifications

General

Wireless

Standards compliance	IEEE 802.11, IEEE 802.11b Direct Sequence Spread Spectrum - DSSS, IEEE 802.11g
RF frequency range	Range 2.4 to 2.4835 GHz, 2.4 to 2.497 GHz for Japan
Data rate	Auto, 11, 5.5, 2, and 1 Mb/s
Modulation	Auto 11 and 5.5 Mb/s = CCK, 2 Mb/s = DQPSK, 1 Mb/s = DBPSK
Number of channels	Europe = 13, Spain = 2, France = 4, US = 11, Japan = 14
Transmit power	17.5 dBm (EIRP)
Receive sensitivity	-83 dBm at 11 Mbps
Router	
Ethernet standards compliance	IEEE 802.3, IEEE 802.3u
Number of ports	One
Number of uplink ports	One
Electrical	
Input voltage range	100 – 240 VAC, 50 – 60 Hz
Power consumption	5 watts
Environmental	
Operating temperature	0° C – 40° C, -150 to 10000 ft.
Storage temperature	-30° C to 80° C
Humidity	5 to 95% RH, non-condensing
Antenna	Two fixed; one internal and one external
LED Indicators	
Modem	Receive, Send, Online, Internet
Access point	Wireless
Other	Power
Interfaces	(1) AC Power, (1) F-Type, (1) RJ-45 (1) USB Series B
Dimensions	47.0 W x 149.1 D x 218.2 H (mm)
Weight	485 g (15.6 oz. — unit only)

Cable Modem

Downstream

Modulation	64 QAM or 256 QAM
Maximum data rate	38 Mbps
Frequency	88 MHz to 860 MHz (30 kHz minimum step size)
Bandwidth	6 MHz
Maximum symbol rate	5.069 Msym/s (64 QAM) 5.361 Msym/s (256 QAM)
Operating level range	-15 dBmV to +15 dBmV
Input impedance	75 ohms (nominal)
Frequency range	88 to 860 MHz

Upstream

Modulation	QPSK, 16 QAM, 32 QAM, 64 QAM, or 128 QAM
Modulation rate (nominal)	TDMA: 160, 320, 640, 1280, 2560, and 5120 KHz S-CDMA: 1280, 2560, and 5120 KHz
Maximum data rate	30 Mbps
Bandwidth	TDMA: 200, 400, 800, 1600, 3200, and 6400 kHz S-CDMA: 1600, 3200, and 6400 kHz
Frequency	5 MHz to 42 MHz (edge to edge)
Symbol rates	160, 320, 640, 1280, and 2560 ksym/s
Operating level range (one channel)	TDMA: • +8 dBmV to +54 dBmV (32 QAM, 64 QAM) • +8 dBmV to +55 dBmV (8 QAM, 16 QAM) • +8 dBmV to +58 dBmV (QPSK) S-CDMA: • +8 dBmV to +53 dBmV (all modulations)
Output impedance	75 ohms nominal
Output return loss	> 6 dB (5 to 42 MHz)

General

Cable interface	F-Connector, female, 75 ohm
CPE network interface	USB, Ethernet 10/100Base-T (auto sensing)
Data protocol	TCP/IP

Glossary

This glossary defines terms and lists acronyms used with the SBG900.

To return to your previous page, click the Acrobat Go to Previous View button.

A

access point A device that provides wireless LAN connectivity to wireless clients (stations). The SBG900 acts as a wireless access point.

adapter A device or card that connects a computer, printer, or other peripheral device to the network or to some other device. A *wireless adapter* connects a computer to the wireless LAN.

address translation See *NAT*.

ALG Application level gateway triggers are required by some file transfer (for example, FTP), game, and video conferencing applications to open one or more ports to enable the application to operate properly.

American Wire Gauge (AWG) A standard system used to designate the size of electrical conductors; gauge numbers are inverse to size.

ANSI The American National Standards Institute is a non-profit, independent organization supported by trade organizations, industry, and professional societies for standards development in the United States. This organization defined ASCII and represents the United States to the International Organization for Standardization.

ANX Automotive Network Exchange

ARP Address Resolution Protocol broadcasts a datagram to obtain a response containing a MAC address corresponding to the host IP address. When it is first connected to the network, a client sends an ARP message. The SBG900 responds with a message containing its MAC address. Subsequently, data sent by the computer uses the SBG900 MAC address as its destination.

ASCII The American Standard Code for Information Interchange refers to alphanumeric data for processing and communication compatibility among various devices; normally used for asynchronous transmission.

asynchronous timing The SBG900 uses synchronous timing for upstream data transmissions. The CMTS broadcasts messages that bandwidth is available. The SBG900 reserves data bytes requiring x-number of mini-slots. The CMTS replies that it can receive data at a specified time (synchronized). At the specified time, the SBG900 transmits the x-number of data bytes.

attenuation The difference between transmitted and received power resulting from loss through equipment, transmission lines, or other devices; usually expressed in decibels.

authentication A process where the CMTS verifies that access is authorized, using a password, trusted IP address, or serial number.

authorization Part of the process between a CMTS and the cable modem or gateway to enable Baseline Privacy.

auto-MDIX Automatic medium-dependent interface crossover detects and corrects cabling errors by automatically reversing the send and receive pins on any port. It enables the use of straight-through wiring between the SBG900 Ethernet port and any computer, printer, or hub.

To return to your previous page, click the Acrobat Go to Previous View button.

B

bandwidth The transmission capacity of a medium in terms of a range of frequencies. Greater bandwidth indicates the ability to transmit more data over a given period of time.

Baseline Privacy An optional feature that encrypts data between the CMTS and the cable modem or gateway. Protection of service is provided by ensuring that a cable modem or gateway, uniquely identified by its MAC address, can only obtain keys for services it is authorized to access.

baud The analog signaling rate. For complex modulation modes, the digital bit rate is encoded in multiple bits per baud, for example, 64 QAM encodes 6 bits per baud and 16 QAM encodes 4 bits per baud.

BCP Binary Communication Protocol

BER The bit error rate is the ratio of the number of erroneous bits or characters received from some fixed number of bits transmitted.

binary A numbering system that uses two digits, 0 and 1.

bit rate The number of bits (digital 0s and 1s) transmitted per second in a communications channel. It is usually measured in bits per second bps.

BPKM Baseline Protocol Key Management encrypts data flows between a cable modem or gateway and the CMTS. The encryption occurs after the cable modem or gateway registers to ensure data privacy across the RF network.

bps bits per second

bridge An OSI layer 2 networking device that connects two LANs using similar protocols. It filters frames based on the MAC address to reduce the amount of traffic. A bridge can be placed between two groups of hosts that communicate a lot together, but not so much with the hosts in the other group. The bridge examines the destination of each packet to determine whether to transmit it to the other side. See also *switch*.

broadband High bandwidth network technology that multiplexes multiple, independent carriers to carry voice, video, data, and other interactive services over a single cable. A communications medium that can transmit a relatively large amount of data in a given time period. A frequently used synonym for cable TV that can describe any technology capable of delivering multiple channels and services.

broadcast Simultaneous transmission to multiple network devices; a protocol mechanism supporting group and universal addressing. See also *multicast* and *unicast*.

To return to your previous page, click the Acrobat Go to Previous View button.

C

CableHome A project of CableLabs and technology suppliers to develop interface specifications for extending high-quality cable-based services to home network devices. It addresses issues such as device interoperability, QoS, and network management. CableHome will enable cable service providers to offer more services over HFC. It will improve consumer convenience by providing cable-delivered services throughout the home.

CableLabs A research consortium that defines the interface requirements for cable modems and acknowledges that tested equipment complies with DOCSIS.

cable modem A device installed at a subscriber location to provide data communications over an HFC network. Unless otherwise specified, all references to “cable modem” in this documentation refers to DOCSIS or Euro-DOCSIS cable modems *only*.

cable modem configuration file File containing operational parameters that a cable modem or gateway downloads from the cable service provider TFTP server during registration.

circuit-switched Network-connection scheme used in the traditional PSTN telephone network where each connection requires a dedicated path for its duration. An alternative is packet-switched.

Class C network An IP network containing up to 253 hosts. Class C IP addresses are in the form “network.network.network.host.”

client In a client/server architecture, a client is a computer that requests files or services such as file transfer, remote login, or printing from the server. Also called a CPE.

On a wireless LAN, a client is any host that can communicate with the access point. A wireless client is also called a “station.”

CMTS A cable modem termination system is a device in the cable system headend that interfaces the HFC network to local or remote IP networks to connecting IP hosts, cable modems or gateways, and subscribers. It manages all cable modem bandwidth. It is sometimes called an edge router.

CNR carrier to noise ratio

coaxial cable (coax) A type of cable consisting of a center wire surrounded by insulation and a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. Coaxial cable has high bandwidth and can support transmission over long distances.

CoS Class of service traffic management or scheduling functions are performed when transferring data upstream or downstream on HFC.

CPE Customer premise equipment, typically computers, printers, etc., are connected to the cable modem or gateway at the subscriber location. CPE can be provided by the subscriber or the cable service provider. Also called a client.

crosstalk Undesired signal interfering with the desired signal.

CSMA/CD carrier sense multiple access with collision detection

To return to your previous page, click the Acrobat Go to Previous View button.

D

datagram In RFC 1594, a datagram is defined as “a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.” For the most part, it has been replaced by the term packet.

default route The route by which packets are forwarded when other routes in the routing table do not apply.

dB decibel

dBc Signal level expressed in dB relative to the unmodulated carrier level desired.

DBm A unit of measurement referenced to one milliwatt across specified impedance. 0dBm = 1 milliwatt across 75 ohms.

dBmV Signal level expressed in dB as the ratio of the signal power in a 75-ohm system to a reference power when 1 mV is across 75 ohms.

demodulation An operation to restore a previously modulated wave and separate the multiple signals that were combined and modulated on a subcarrier.

DHCP A Dynamic Host Configuration Protocol server dynamically assigns IP addresses to client hosts on an IP network. DHCP eliminates the need to manually assign static IP addresses by “leasing” an IP address and subnet mask to each client. It enables the automatic reuse of unused IP addresses:

The SBG900 is simultaneously a DHCP client and a DHCP server.

- A DHCP server at the cable system headend assigns a public IP address to the SBG900 and optionally to clients on the SBG900 LAN.
- The SBG900 contains a built-in DHCP server that assigns private IP addresses to clients.

distortion An undesired change in signal waveform within a transmission medium. A nonlinear reproduction of the input waveform.

DMZ A “de-militarized zone” is one or more hosts logically located between a private LAN and the Internet. A DMZ prevents direct access by outside users to private data. (The term comes from the geographic buffers located between some conflicting countries such as North and South Korea.) In a typical small DMZ configuration, the DMZ host receives requests from private LAN users to access external web sites and initiates sessions for these requests. The DMZ host cannot initiate a session back to the private LAN. Internet users outside the private LAN can access only the DMZ host. You can use a DMZ to set up a web server or for gaming without exposing confidential data.

DNS The Domain Name System is the Internet system for converting domain names to IP addresses. A DNS server contains a table matching domain names such as Internetname.com to IP addresses such as 192.169.9.1. When you access the world-wide web, a DNS server translates the URL displayed on the browser to the destination website IP address. The DNS lookup table is a distributed Internet database; no one DNS server lists all domain name to IP address matches.

DOCSIS The CableLabs Data-Over-Cable Service Interface Specification defines interface standards for cable modems, gateways, and supporting equipment to deliver data between an HFC network and a computer systems or television sets. To emphasize its use as a cable modem standard, DOCSIS is now called CableLabs Certified Cable Modems. Euro-DOCSIS is DOCSIS adapted for use in Europe.

domain name A unique name, such as motorola.com, that maps to an IP address. Domain names are typically much easier to remember than are IP addresses.

To return to your previous page, click the Acrobat Go to Previous View button.

dotted-decimal format	Method of representing an IP address or subnet mask using four decimal numbers called octets. Each octet represents eight bits. In a class C IP address, the octets are “network.network.network.host.” The first three octets together represent the network address and the final octet is the host address. In the SBG900 LAN default configuration, 192.168.100 represents the network address. In the final octet, the host address can be from 2 to 254.
download	To copy a file from one computer to another. You can use the Internet to download files from a server to a computer. A DOCSIS or Euro-DOCSIS cable modem or gateway downloads its configuration file from a TFTP server during start-up.
downstream	In a cable data network, the direction of data received by the computer from the Internet.
driver	Software that enables a computer to interact with a network or other device. For example, there are drivers for printers, monitors, graphics adapters, modems, Ethernet, USB, HPNA, and many others.
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum is an IEEE 802.11b RF modulation protocol.
dynamic IP address	An IP address that is temporarily leased to a host by a DHCP server. The opposite of *static IP address*.

E

encapsulate	To include data into some other data unit to hide the format of the included data.
encode	To alter an electronic signal so that only an authorized user can unscramble it to view the information.
encrypt	To encode data.
endpoint	A VPN endpoint terminates the VPN at the router so that computers on the SBG900 LAN do not need VPN client software to tunnel through the Internet to the VPN server.
ESSID	The Extended Service Set Identifier or network name is a unique identifier that wireless clients use to associate with an access point to distinguish between multiple wireless LANs in the same area. All clients on a wireless LAN must have the same ESSID as the access point. On the SBG900, you can set the ESSID on the Wireless > NETWORK page.
Ethernet	The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides speeds up to 100 Mbps. “Base” means “baseband technology” and “T” means “twisted pair cable.”’ Each Ethernet port has a physical address called the MAC address.
Euro-DOCSIS	A tComLabs standard that is DOCSIS adapted for use in Europe
event	A message generated by a device to inform an operator or the network management system that something has occurred.
expansion slot	A connection point in a computer where a circuit board can be inserted to add new capabilities.

To return to your previous page, click the Acrobat Go to Previous View button.

F

FCS frame check sequence

F-type connector A type of connector used to connect coaxial cable to equipment such as the SBG900.

firewall A security software system on the SBG900 that enforces an access control policy between the Internet and the SBG900 LAN.

flow A data path moving in one direction.

FEC Forward error correction is a technique to correct transmission errors without requiring the transmitter to resend any data.

FDMA Frequency Division Multiple Access is a method to allow multiple users to share a specific radio spectrum. Each active user is assigned an individual RF channel (or carrier) with the carrier frequency of each channel offset from its adjacent channels by an amount equal to the channel spacing, which allows the required bandwidth per channel.

frame A unit of data transmitted between network nodes that contains addressing and protocol control data. Some control frames contain no data.

frequency Number of times an electromagnetic signal repeats an identical cycle in a unit of time, usually one second, measured in Hz, kHz, MHz, or GHz.

FTP File Transfer Protocol is a standard Internet protocol for exchanging files between computers. FTP is commonly used to download programs and other files to a computer from web pages on Internet servers.

full-duplex The ability to simultaneously transmit and receive data. See also *half-duplex*.

G

gateway A device that enables communication between networks using different protocols. See also *router.*

The SBG900 enables up to 253 computers supporting IEEE 802.11b, Ethernet, or USB to share a single broadband Internet connection.

gateway IP address The address of the default gateway router on the Internet. Also known as the “giaddr.”

GHz Gigahertz — one billion cycles per second.

GUI graphical user interface

To return to your previous page, click the Acrobat Go to Previous View button.

H

H.323 A suite of protocols created by the ITU for interactive video-conferencing, data sharing, and audio applications such as VoIP.

half-duplex Network where only one device at a time can transmit data. See also *full-duplex*.

headend A location that receives TV programming, radio programming, data, and telephone calls that it modulates onto the HFC network. It also sends return data and telephone transmissions. Headend equipment includes transmitters, preamplifiers, frequency terminals, demodulators, modulators, and other devices that amplify, filter, and convert incoming broadcast TV signals to wireless and cable channels.

header The data at the beginning of a packet that identifies what is in the packet.

hexadecimal A base-sixteen numbering system that uses sixteen sequential numbers (0 to 9 and the letters A to F) as base units before adding a new position. On computers, hexadecimal is a convenient way to express binary numbers.

HFC A hybrid fiber/coaxial cable network uses fiber-optic cable as the trunk and coaxial cable to the subscriber premises.

hop The interval between two routers on an IP network. The number of hops a packet traverses toward its destination (called the hop count) is saved in the packet header. For example, a hop count of six means the packet has traversed six routers. The packet hop count increases as the time-to-live (TTL) value decreases.

host In IP, a host is any computer supporting end-user applications or services with full two-way network access. Each host has a unique host number that combined with the network number forms its IP address.

Host also can mean:

- A computer running a web server that serves pages for one or more web sites belonging to organization(s) or individuals
- A company that provides this service
- In IBM environments, a mainframe computer

HTML Hyper Text Markup Language

hub On a LAN, a hub is a device that connects multiple hosts to the LAN. A hub performs no data filtering. See also *bridge* and *router*. An IP hub is typically a unit on a rack or desktop.

On an HFC network, a hub is a scaled-down headend that performs some or all headend functions for part of the system.

Hz Hertz — one cycle per second. The unit to measure the frequency that an alternating electromagnetic signal cycles through its highest and lowest states. Used to define the bands of the electromagnetic spectrum used in voice and data communications, or to define the bandwidth of a transmission medium.

To return to your previous page, click the Acrobat Go to Previous View button.

I

IANA The Internet Numbering Address Authority (IANA) is an organization under the Internet Architecture Board (IAB) of the Internet Society that oversees IP address allocation. It is under a contract from the U.S. government.

ICMP Internet Control Message Protocol is a protocol used for error, problem, and informational messages sent between IP hosts and gateways. ICMP messages are processed by the IP software and are not usually apparent to the end-user.

ICSA The International Computer Security Association is the security industry's main source of research, intelligence, and product certification.

IEEE The Institute of Electrical and Electronics Engineers, Inc. (http://www.ieee.org) is an organization that produces standards, technical papers, and symposiums for the electrical and electronic industries and is accredited by ANSI.

IEEE 802.11b
IEEE 802.11g IEEE wireless network standards.

IEEE 802.3 See *Ethernet*.

IETF The Internet Engineering Task Force (http://www.ietf.org) is an open international community of network designers, operators, vendors, and researchers to develop and maintain Internet architecture. Technical working groups issue working documents called Internet-Drafts. The IETF publishes review versions of the drafts called requests for comments (RFCs).

IGMP Internet Group Membership Protocol the Internet multicasting standard. IGMP establishes and maintains a database of group multicast addresses and interfaces to which a multicast router forwards multicast packets. IGMP runs between multicast hosts and their immediately-neighboring multicast routers.

IGMP spoofing A process where a router acts as an IGMP querier for multicast hosts and an IGMP host to a multicast router.

impedance The total opposition to ac electron current flow within a device. Impedance is typically 75 ohms for coax cable and other CATV components.

impulse noise Noise of very short in duration, typically of the order of 10 microseconds. It is caused by electrical transients such as voltage spikes, electric motors turning on, and lightning or switching equipment that bleed over to the cable.

ingress noise Noise typically caused by discrete frequencies picked up by the cable plant from radio broadcasts or an improperly grounded or shielded home appliance such as a hair dryer. Ingress is the major source of cable system noise.

Internet A worldwide collection of interconnected networks using TCP/IP.

Internetwork A collection of interconnected networks allowing communication between all devices connected to any network in the collection.

IP Internet Protocol is a set of standards that enable different types of computers to communicate with one another and exchange data through the Internet. IP provides the appearance of a single, seamless communication system and makes the Internet a virtual network.

To return to your previous page, click the Acrobat Go to Previous View button.

IP address A unique 32-bit value that identifies each host on a TCP/IP network. TCP/IP networks route messages based on the destination IP address. An IP address has two parts:

- The network address is assigned by IANA.
- The SBG900 network administrator assigns a host address to each host connected to the SBG900, automatically using its DHCP server or as a static IP address.

For a Class C network, the first 24 bits are the network address and the final 8 bits are the host address; in dotted-decimal format it appears “network.network.network.host.”

If you enable the SBG900 DHCP client on the WAN page, the cable service provider automatically assigns the network address, subnet mask, domain name, and DNS server to provide a continuous Internet connection.

IPSec The Internet Protocol Security protocols are IETF authentication and encryption standards for secure packet exchange over the Internet. IPSec works at OSI layer 3 and secures everything on the network.

IKE Internet Key Exchange

ISAKMP Internet Security Association and Key Management Protocol

ISDN Integrated Services Digital Network

ISO The International Organization for Standardization (http://www.iso.ch) is a worldwide federation of national standards bodies from approximately 140 countries. ISO is a non-governmental organization established in 1947 to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity.

ISP Internet Service Provider

ITU International Telecommunications Union

K

kHz kilohertz — one thousand cycles per second

To return to your previous page, click the Acrobat Go to Previous View button.

L

L2F Layer 2 Forwarding is an OSI layer 2 protocol that establishes a secure tunnel across the Internet to create a virtual PPP connection between the user and the enterprise network. L2F is the most established and stable layer 2 tunneling protocol.

L2TP Layer 2 Tunnel Protocol is a PPP extension that enables ISPs to operate VPNs. L2TP merges the best features of the PPTP and L2F. L2TP is the emerging IETF standard.

LAC An L2TP access concentrator is a device to which the client directly connects through which PPP frames are tunneled to the LNS. The LAC need only implement the media over which L2TP operates to transmit traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F NAS.

LAN A local area network provides a full-time, high-bandwidth connection over a limited area, such as a building or campus. Ethernet is the most widely used LAN standard.

layer In networks, layers are software protocol levels. Each layer performs functions for the layers above it. OSI is a reference model having seven functional layers.

LCP Link Control Protocol establishes, configures, and tests data link connections used by PPP.

latency The time required for a signal to pass through a device. It is often expressed in a quantity of symbols.

LED light-emitting diode

LNS An L2TP network server is a termination point for L2TP tunnels where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single media over which L2TP tunnels arrive. The LNS can have a single LAN or WAN interface but can terminate calls arriving at any of the LACs full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.

loopback A test that loops the transmit signal to the receive signal. Usually the loopback test is initiated on a network device. The test is used to verify a path or to measure the quality of a signal on that path.

To return to your previous page, click the Acrobat Go to Previous View button.

M

MAC address The Media Access Control address is a unique, 48-bit value permanently saved in ROM at the factory to identify each Ethernet network device. It is expressed as a sequence of 12 hexadecimal digits printed on a Label on the Bottom of the SBG900. You need to provide the HFC MAC address to the cable service provider.
Also called an Ethernet address, physical address, hardware address, or NIC address.

MB One megabyte; equals 1,024 x 1,024 bytes, 1,024 kilobytes, or about 8 million bits.

Mbps Million bits per second (megabits per second). A rate of data transfer.

media The various physical environments through which signals pass; for example, coaxial, unshielded twisted-pair (UTP), or fiber-optic cable.

MIB A management information base is a unique hierarchical structure of software objects used by the SNMP manager and agent to configure, monitor, or test a device.

MHz Megahertz — one million cycles per second. A measure of radio frequency.

MPDU MAC protocol data unit (PDU)

MSDU MAC service data unit

MSO Multiple Systems Operator. A company that owns and operates more than one cable system. Also called a group operator.

MTU The Maximum Transmission Unit is the largest amount of data that can be transmitted in one discrete message on a given physical network. The MTU places an upper bound on the size of a message that can be transferred by the network in a single frame. Messages exceeding the MTU must be fragmented before transmission, and reassembled at the destination.

multicast A data transmission sent from one sender to multiple receivers. See also *broadcast* and *unicast*.

mW milliwatts

To return to your previous page, click the Acrobat Go to Previous View button.

N

NAS network access server

NAT Network Address Translation is an Internet standard for a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. NAT provides some security because the IP addresses of SBG900 LAN computers are invisible on the Internet.

If NAT is enabled on the Gateway page, there is a one-to-one mapping between each public IP address and client IP address.

NAPT Network Address Port Translation is the most common form of address translation between public and private IP addresses. NAPT is a mapping of one public IP address to many private IP addresses. If NAPT is enabled on the Gateway page, one public IP address is mapped to an individual private IP address for up to 245 LAN clients.

NEC National Electrical Code (United States) — The regulations for construction and installation of electrical wiring and apparatus, suitable for mandatory application by a wide range of state and local authorities.

network Two or more computers connected to communicate with each other. Networks have traditionally been connected using some kind of wiring.

network driver Software packaged with a NIC that enables the computer to communicate with the NIC.

network layer Layer 3 in the OSI architecture that provides services to establish a path between open systems. The network layer knows the address of the neighboring nodes, packages output with the correct network address data, selects routes, and recognizes and forwards to the transport layer incoming messages for local host domains.

NIC A network interface card converts computer data to serial data in a packet format that it sends over the LAN. A NIC is installed in an expansion slot or can be built-in. Every Ethernet NIC has a MAC address permanently saved in its ROM.

node On a LAN, a generic term for any network device.

On an HFC network, the interface between the fiber-optic trunk and coaxial cable feeders to subscriber locations. A node is typically located in the subscriber neighborhood.

noise Random spurts of electrical energy or interface. May produce a salt-and-pepper pattern on a television picture.

O

ohm A unit of electrical resistance.

OSI The Open Systems Interconnection reference model is an illustrative model describing how data moves from an application on the source host through a network to an application on the destination host. It is a conceptual framework developed by ISO that is now the primary model for intercomputer communications. OSI is a model *only*; it does not define a specific networking interface.

To return to your previous page, click the Acrobat Go to Previous View button.

P

packet The unit of data that is routed between the sender and destination on the Internet or other packet-switched network. When data such as an e-mail message or other file is sent over the Internet, IP on the sender divides the data into uniquely-numbered packets. The packet header contains the source and destination IP addresses. The individual packets may travel different routes. When all packets arrive at the destination, IP at that end reassembles the packets. The header and the data can vary in length. Packet and datagram are similar in meaning.

packet-switched A scheme to handle transmissions on a connectionless network such as the Internet. An alternative is circuit-switched.

PacketCable A CableLabs-led project to define a common platform to deliver advanced real-time multimedia services over two-way HFC cable plant. Built on DOCSIS 1.1, PacketCable networks use IP technology as the basis for a highly-capable multimedia architecture.

pass-through A pass-through client on the SBG900 LAN obtains its public IP address from the cable service provider DHCP server.

PAT Port Address Translation

PCMCIA The Personal Computer Memory Card International Association sets international standards for connecting peripherals to portable computers. Laptop computers typically have a PCMCIA slot that can hold one or two PC Cards to provide features such as Ethernet connectivity.

PDA personal desktop assistant

PDU A protocol data unit is a message containing operational instructions used for SNMP. The basic SNMP V2 PDU types are get-request, get-next-request, get-bulk-request, response, set-request, inform-request, and trap.

periodic ranging Ranging that is performed on an on-going basis after initial ranging has taken place.

physical layer Layer 1 in the OSI architecture. It provides services to transmit bits or groups of bits over a transmission link between open systems. It entails the electrical, mechanical, and handshaking procedures.

piggybacking A process that occurs when a cable modem simultaneously transmits data and requests additional bandwidth.

PING A network utility that tests host reachability by sending a small packet to the host and waiting for a reply. If you PING a computer IP address and receive a reply, you know the computer is reachable over the network. It also stands for “Packet InterNet Groper.”

PMD The physical media-dependent sublayer of the physical layer which transmits bits or groups of bits over particular types of transmission links between open systems. It entails the electrical, mechanical, and handshaking procedures.

point-to-point Physical connection made from one point to another.

POTS The “plain old telephone service” offered through the PSTN; basic analog telephone service. POTS uses the lowest 4 kHz of bandwidth on twisted pair wiring.

port On a computer or other electronic device, a port is a socket or plug used to physically connect it to the network or to other devices.

in TCP/IP, a port is a number from 0 to 65536 used logically by a client program to specify a server program. Ports 0 to 1024 are reserved

To return to your previous page, click the Acrobat Go to Previous View button.

port mirroring A feature that enables one port (source) on the SBG900 to be copied to another port (destination) to be studied. The destination mirrors the transmitted (from) or received (to) data on the source port to enable the person managing the network to monitor activity.

port triggering A mechanism that allows incoming communication with specified applications. Primarily used for gaming applications.

PPP Point-to-Point Protocol is used to transport other protocols, typically for simple links over serial lines. It is most commonly used to access the Internet with a dial-up modem.

PPTP Point-to-Point Tunneling Protocol encapsulates other protocols. It is a new technology to create VPNs developed jointly by several vendors.

private IP address An IP address assigned to a computer on the SBG900 LAN by the DHCP server on the SBG900 for a specified lease time. Private IP addresses are used by the SBG900 LAN only; they are invisible to devices on the Internet. See also *public IP address*.

protocol A formal set of rules and conventions for exchanging data. Different computer types (for example PC, UNIX, or mainframe) can communicate if they support common protocols.

provisioning The process of autodiscovery or manually configuring a cable modem on the CMTS.

PSTN The public switched telephone network is the traditional circuit-switched, voice-oriented telephone network. See also *POTS*.

public IP address The IP address assigned to the SBG900 by the cable service provider. A public IP address is visible to devices on the Internet. See also *private IP address*.

Q

QAM Quadrature Amplitude Modulation uses amplitude and phase modulation to encode multiple bits of data in one signaling element. QAM achieves faster data transfer than amplitude or phase modulation alone, but the signal is more prone to errors caused by noise. QAM requires a transmission circuit with a higher CNR than alternate modulation formats such as QPSK. Two types of QAM are:

- 16 QAM encodes four bits per symbol as one of 16 possible amplitude and phase combinations.
- 64 QAM encodes six bits per symbol as one of 64 possible amplitude and phase combinations.

QPSK Quadrature Phase Shift Key (QPSK) modulation sends two bits of information per symbol period with one symbol 90 degrees out of phase with other symbols. The four constellation points represented by the coordinates (0,0 - 0,1 - 1,0 - 1,1) represent the four possible combinations.

QoS Quality of service describes the priority, delay, throughput, and bandwidth of a connection.

To return to your previous page, click the Acrobat Go to Previous View button.

R

RAS Remote Access Server

registration How a cable modem makes itself known to the CMTS. The cable modem configuration file and authorization are verified and the CoS is negotiated.

return loss A measurement of the quality of the match of the device to the cable system. Return loss is the ratio of the amount of power reflected by the device. A return loss of 20 dB or greater is preferred.

RF Radio Frequency — signals used by the CMTS transmitter and receiver to send data over HFC. The carrier is modulated to encode the digital data stream for transmission across the cable network.

RFC Request for Comments published on the IETF or other websites. Many RFCs become international standards.

RJ-11 The most common type of connector for household or office phones.

RJ-45 An 8-pin modular connector; the most common connector type for 10Base-T or 100Base-T Ethernet networks.

ROM read-only memory

router On IP networks, a device connecting at least two networks, which may or may not be similar. A router is typically located at a *gateway* between networks. A router operates on OSI network layer 3. It filters packets based on the IP address, examining the source and destination IP addresses to determine the best route on which to forward them.

A router is often included as part of a network switch. A router can also be implemented as software on a computer.

routing table A table listing available routes that is used by a router to determine the best route for a packet.

RTS request to send

To return to your previous page, click the Acrobat Go to Previous View button.

S

server	In a client/server architecture, a dedicated computer that supplies files or services such as file transfer, remote login, or printing to clients.
scope	The set of IP addresses that a DHCP server can lease to clients.
service provider	A company providing cable data services to subscribers.
SID	A service ID is a unique 14-bit identifier the CMTS assigns to a cable modem or gateway that identifies the traffic type it carries (for example, data or voice). The SID provides the basis for the CMTS to allocate bandwidth to the cable modem and implement CoS.
SDU	service data unit
SME	small and medium enterprise
SMTP	Simple Mail Transfer Protocol is a standard Internet protocol for transferring e-mail.
SNMP	Simple Network Management Protocol is a standard to monitor and manage networks and network devices. Data is exchanged using PDU messages.
SOHO	small office home office
spectrum	A specified range of frequencies used for transmission of electromagnetic signals.
spectrum allocation	An allocation of portions of the available electromagnetic spectrum for specific services, such as AM, FM, or personal communications.
splitter	A device that divides the signal from an input cable between two or more cables.
stateful inspection	A type of firewall that tracks each connection traversing all firewall interfaces to ensure validity. In addition to examining the source and destination in the packet header based on static rules, a stateful inspection firewall: • Examines packet headers on context established by previous packets that traversed the firewall • Monitors the connection state and saves it in a table • Closes ports until a connection to a specific port is requested • May examine the packet contents up through the application layer to determine more than just the source and destination A stateful-inspection firewall is more advanced than a static filter firewall.
static filter	A type of firewall that examines the source and destination in the packet header based on administrator-defined rules *only*.
static IP address	An IP address that is permanently assigned to a host. Normally, a static IP address must be assigned manually. The opposite of dynamic IP address.
static route	A manually-defined route.
station	IEEE 802.11b term for wireless client.
subscriber	A home or office user who accesses television, data, or other services from a cable service provider.
subnet mask	A bit mask that is logically ANDed with the destination IP address of a packet to determine the network address. A router routes packets using the network address.
subnetwork	A part of a network; commonly abbreviated “subnet.” When subnetting is used, the host portion of the IP address is divided into a subnet and host number. Hosts and routers use the subnet mask to identify the bits used for the network and subnet number.

To return to your previous page, click the Acrobat Go to Previous View button.

switch	On an Ethernet network, a switch filters frames based on the MAC address, in a manner similar to a bridge. A switch is more advanced because it can connect more than two segments.
symbol rate	Also known as baud rate, is a measure of the number of times per second a signal in a communications channel varies, or makes a transition between states (states being frequencies, voltage levels or phase angles). Usually measured in symbols per second (sps).
SYSLOG	A de-facto UNIX standard for logging system events.

T

TBCP	Tagged Binary Communication Protocol
TCP	Transmission Control Protocol on OSI transport layer four, provides reliable transport over the network for data transmitted using IP (network layer three). It is an end-to-end protocol defining rules and procedures for data exchange between hosts on top of connectionless IP. TCP uses a timer to track outstanding packets, checks error in incoming packets, and retransmits packets if requested.
TCP/IP	The Transmission Control Protocol/Internet Protocol suite provides standards and rules for data communication between networks on the Internet. It is the worldwide internetworking standard and the basic communications protocol of the Internet.
TFTP	Trivial File Transfer Protocol is a very simple protocol used to transfer files.
transparent bridging	A method to enable all hosts on the wired Ethernet LAN, wireless LAN, and USB connection to communicate as if they were all connected to the same physical network.
transport layer	Layer of the OSI concerned with protocols for error recognition and recovery. This layer also regulates information flow.
trunk	Electronic path over which date is transmitted.
TTL	The time to live is the number of routers (or hops) a packet can traverse before being discarded. When a router processes a packet, it decreases the TTL by 1. When the TTL reaches zero, the packet is discarded.
tunnel	To place packets inside other packets to send over a network. The protocol of the enclosing packet is understood by each endpoint, or tunnel interface, where the packet enters and exits the network. VPNs rely on tunneling to create a secure network. Tunneling requires the following protocol types: • A carrier protocol, such as TCP, used by the network that the data travels over • An encapsulating protocol, such as IPSec, L2F, L2TP, or PPTP, that is wrapped around the original data • A passenger protocol, such as IP, for the original data
two-way	A cable system that can transmit signals in both directions to and from the headend and the subscriber.

To return to your previous page, click the Acrobat Go to Previous View button.

U-Z

UDP	User Datagram Protocol
unicast	A point-to-point data transmission sent from one sender to one receiver. This the normal way you access websites. See also *broadcast* and *multicast*.
upstream	In a cable data network, upstream describes the direction of data sent from the subscriber computer through the cable modem to the CMTS and the Internet.
USB	Universal Serial Bus is a computer interface for add-on devices such as printers, scanners, mice, modems, or keyboards. USB supports data transfer rates of 12 Mbps and plug-and-play installation. You can connect up to 127 devices to a single USB port.
UTP	unshielded twisted pair (wire)
VLAN	A virtual local area network is group of devices on different LAN segments that are logically configured to communicate as if they are connected to the same wire.
VoIP	Voice over Internet Protocol is a method to exchange voice, fax, and other information over the Internet. Voice and fax have traditionally been carried over traditional telephone lines of the PSTN using a dedicated circuit for each line. VoIP enables calls to travel as discrete data packets on shared lines. VoIP is an important part of the convergence of computers, telephones, and television into a single integrated information network.
VPN	A virtual private network is a private network that uses “virtual” connections (tunnels) routed over a public network (usually the Internet) to provide a secure and fast connection; usually to users working remotely at home or in small branch offices. A VPN connection provides security and performance similar to a dedicated link (for example, a leased line), but at much lower cost.
WAN	A wide-area network provides a connection over a large geographic area, such as a country or the whole world. The bandwidth depends on need and cost, but is usually much lower than for a LAN.
WAP	Wireless access point or Wireless Access Protocol. See also *access point*.
WECA	The Wireless Ethernet Compatibility Alliance is a trade organization that works to ensure that all wireless devices — computer cards, laptops, air routers, PDAs, etc — can communicate with each other.
WEP	Wired Equivalent Privacy encryption protects the privacy of data transmitted over a wireless LAN. WEP uses keys to encrypt and decrypt transmitted data. The access point must authenticate a client before it can transfer data to another client. WEP is part of IEEE 802.11b.
WiFi	Wireless fidelity (pronounced y-phi) brand name applied to products supporting IEEE 802.11b.
Wireless Cable Modem Gateway	The Motorola SURFboard Wireless Cable Modem Gateway is a single device that combines a cable modem, router, Ethernet switch, wireless access point, and DHCP server for SOHO or SME use.
WLAN	wireless LAN
world wide web	An interface to the Internet that you use to navigate and hyperlink to information.

To return to your previous page, click the Acrobat Go to Previous View button.

Software License

Motorola, Inc., Broadband Communications Sector ("Motorola"), 101 Tournament Drive, Horsham, PA 19044

IMPORTANT: PLEASE READ THIS SOFTWARE LICENSE ("LICENSE") CAREFULLY BEFORE YOU INSTALL, DOWNLOAD OR USE ANY APPLICATION SOFTWARE, USB DRIVER SOFTWARE, FIRMWARE AND RELATED DOCUMENTATION ("SOFTWARE") PROVIDED WITH MOTOROLA'S CABLE DATA PRODUCT (THE "CABLE DATA PRODUCT"). BY USING THE CABLE DATA PRODUCT AND/OR INSTALLING, DOWNLOADING OR USING ANY OF THE SOFTWARE, YOU INDICATE YOUR ACCEPTANCE OF EACH OF THE TERMS OF THIS LICENSE. UPON ACCEPTANCE, THIS LICENSE WILL BE A LEGALLY BINDING AGREEMENT BETWEEN YOU AND MOTOROLA. THE TERMS OF THIS LICENSE APPLY TO YOU AND TO ANY SUBSEQUENT USER OF THIS SOFTWARE.

IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE (I) DO NOT INSTALL OR USE THE SOFTWARE AND (II) RETURN THE CABLE DATA PRODUCT AND THE SOFTWARE (COLLECTIVELY, "PRODUCT"), INCLUDING ALL COMPONENTS, DOCUMENTATION AND ANY OTHER MATERIALS PROVIDED WITH THE PRODUCT, TO YOUR POINT OF PURCHASE OR SERVICE PROVIDER, AS THE CASE MAY BE, FOR A FULL REFUND.

The Software includes associated media, any printed materials, and any "on-line" or electronic documentation, as well as any updates, revisions, bug fixes, or drives obtained by you from Motorola or your service provider. Software provided by third parties may be subject to separate end-user license agreements from the manufacturers of such Software.

The Software is never sold. Motorola licenses the Software to the original customer and to any subsequent licensee for personal use only on the terms of this License. Motorola and its 3rd party licensors retain the ownership of the Software.

You may:

USE the Software only in connection with the operation of the Product.

TRANSFER the Software (including all component parts and printed materials) permanently to another person, but only if the person agrees to accept all of the terms of this License. If you transfer the Software, you must at the same time transfer the Product and all copies of the Software (if applicable) to the same person or destroy any copies not transferred.

TERMINATE this License by destroying the original and all copies of the Software (if applicable) in whatever form.

You may not:

(1) Loan, distribute, rent, lease, give, sublicense or otherwise transfer the Software, in whole or in part, to any other person, except as permitted under the TRANSFER paragraph above. (2) Copy or translate the User Guide included with the Software, other than for personal use. (3) Copy, alter, translate, decompile, disassemble or reverse engineer the Software, including but not limited to, modifying the Software to make it operate on non-compatible hardware. (4) Remove, alter or cause not to be displayed, any copyright notices or startup message contained in the Software programs or documentation. (5) Export the Software or the Product components in violation of any United States export laws.

The Product is not designed or intended for use in on-line control of aircraft, air traffic, aircraft navigation or aircraft communications; or in design, construction, operation or maintenance of any nuclear facility. MOTOROLA AND ITS 3RD PARTY LICENSORS DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH USES. YOU REPRESENT AND WARRANT THAT YOU SHALL NOT USE THE PRODUCT FOR SUCH PURPOSES.

Title to this Software, including the ownership of all copyrights, mask work rights, patents, trademarks and all other intellectual property rights subsisting in the foregoing, and all adaptations to and modifications of the foregoing shall at all times remain with Motorola and its 3rd party licensors. Motorola retains all rights not expressly licensed under this License. The Software, including any images, graphics, photographs, animation, video, audio, music and text incorporated therein is owned by Motorola or its 3rd party licensors and is protected by United States copyright laws and international treaty provisions. Except as otherwise expressly provided in this License, the copying, reproduction, distribution or preparation of derivative works of the Software, any portion of the Product or the documentation is strictly prohibited by such laws and treaty provisions. Nothing in this License constitutes a waiver of Motorola's rights under United States copyright law.

This License and your rights regarding any matter it addresses are governed by the laws of the Commonwealth of Pennsylvania, without reference to conflict of laws principles. THIS LICENSE SHALL TERMINATE AUTOMATICALLY if you fail to comply with the terms of this License.

Motorola is not responsible for any third party software provided as a bundled application, or otherwise, with the Software.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Product and documentation is provided with RESTRICTED RIGHTS. The use, duplication or disclosure by the Government is subject to restrictions as set forth in subdivision (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at 52.227-7013. The contractor/manufacturer is Motorola, Inc., Broadband Communications Sector, 101 Tournament Drive, Horsham, PA 19044.

Visit our website at:
www.motorola.com

509091-001
10/03
MGBI